

En las instalaciones de la Unidad de Acceso a la Información Pública de **LA ADMINISTRACIÓN NACIONAL DE ACUEDUCTOS Y ALCANTARILLADOS (ANDA)**: En la ciudad de San Salvador, a las quince horas con treinta minutos del día nueve de octubre del año dos mil dieciocho.

La suscrita Oficial de Información **CONSIDERANDO QUE:**

- I) El día miércoles diecinueve de septiembre de dos mil dieciocho, se recibió por medio de solicitud de información en la Unidad de Acceso a la Información Pública de la Administración Nacional de Acueductos y Alcantarillados (en adelante UAIP ANDA), solicitud de información, por parte del ciudadano: _____, quien se identificó por medio de su Documento Único de Identidad número: _____, solicitando lo siguiente: **1) Documentación de normativas legales orgánicas internas y externas vigentes, 2) Organigrama de la Dirección de Tecnologías de la Información sellada y firmada por la máxima autoridad pertinente, 3) Inventario de Software, hardware y recurso humano de la Dirección de Tecnologías de Información, 4) Presupuesto designado a la Dirección de Tecnologías de Información, 5) Historial de incidencias en la Dirección de Tecnologías de Información, por ejemplo ataques a servidores o bajas de los servicios, 6) Esquema de distribución de equipo informático en el Centro de computo de la Dirección de Tecnologías de la Información, 7) Distribución física de las sub-unidades de la Dirección de Tecnologías de la Información, 8) Listado de sistemas informáticos actualmente en producción y desarrollo, 9) Planes de contingencia de la Dirección de Tecnologías de Información con el centro de cómputo.** **NOTA: Centro de cómputo se refiere a las áreas de Call Center y producción/Desarrollo.**
- II) Verificado el cumplimiento de los requisitos establecidos en el Art. 66 de La ley de Acceso a la información Pública (LAIP) y los Artículos 50, 54 del Reglamento de la LAIP, y en cumplimiento a lo establecido en el Artículo 70 de la LAIP, la suscrita transmitió el requerimiento de información a la unidad administrativa competente, con la finalidad de que localicen lo solicitado y comuniquen la manera en que se encuentre disponible y se verifique la clasificación de la información. Por lo que se realizó el proceso de gestión de solicitud de información a las unidades involucradas en generar, administrar y resguardar la información institucional.
- III) En atención a lo solicitado la Dirección de Tecnologías de Información, proporciono la siguiente información: **1) Documentación de normativas legales orgánicas internas y externas vigente: Esta información es OFICIOSA, se encuentra en el PORTAL DE TRANSPARENCIA de la ANDA. 2) Organigrama de la Dirección de Tecnologías de la Información sellada y firmada por la máxima autoridad pertinente: Esta información es OFICIOSA, se encuentra en el PORTAL DE TRANSPARENCIA de la ANDA. 3) Inventario de Software, hardware y recurso humano de la Dirección de Tecnologías de Información: En base al Artículo 19 literal b) de la Ley de Acceso a la Información Pública, esta información se clasifica como RESERVADA, la cual se encuentra incluida en el índice de información reservada en el acápite 1, R-010-2018 Protocolos y planes de operaciones de seguridad de ANDA a nivel nacional. 4) Presupuesto designado a la Dirección de Tecnologías de Información: El presupuesto vigente designado para dicha unidad es de \$1,055,700.00 (Un millón cincuenta y cinco mil setecientos 00/100 USD), 5) Historial de incidencias en la Dirección de Tecnologías de Información, por ejemplo ataques a servidores o bajas de los servidores: En base al Artículo 19 litera b) de la Ley de Acceso a la Información Pública, esta información se clasifica como RESERVADA, la cual se encuentra concatenada en el índice de información reservada en el acápite 1, R-01-2018 Protocolos y planes de operaciones de seguridad de ANDA a nivel nacional 6) Esquema de distribución de equipo informático en el Centro de computo de la Dirección de Tecnologías de la Información: En base al Artículo 19 literal b) de la Ley de Acceso a la Información Pública, esta información se clasifica como RESERVADA, la cual se encuentra incluida en el índice de información reservada en el acápite 1, R-01-2018 Protocolos y planes de operaciones de seguridad de ANDA a nivel nacional, 7) Distribución física de las sub-unidades de la Dirección de Tecnologías de la Información: En base al Artículo 19 literal b) de la Ley de Acceso a la Información Pública, esta información se clasifica como RESERVADA, la cual se encuentra concatenada en el índice de información reservada en el acápite 1, R-01-2018 Protocolos y planes de operaciones de seguridad de ANDA a nivel nacional, 8) Listado de sistemas informáticos actualmente en producción y desarrollo: En base al Artículo 19 literal b) de la Ley de Acceso a la Información Pública, esta información se clasifica como RESERVADA, la cual se encuentra incluida en el índice de información reservada en el acápite 1, R-01-2018 Protocolos y planes de operaciones de seguridad de ANDA a nivel nacional, 9) Planes de contingencia de la Dirección de Tecnologías de Información con el centro de cómputo: En base al Artículo 19 literal b) de la Ley de Acceso a la Información Pública, esta información se clasifica como RESERVADA, la cual se encuentra incluida en el índice de información reservada en el acápite 1, R-01-2018 Protocolos y planes de operaciones de seguridad de ANDA a nivel nacional.**

- **Las razones por las cuales la información solicitada en los numerales 3,5,6,7,8 y 9 se encuentra en el índice de reserva se expone a continuación: La Dirección de Tecnologías de Información, tiene**

entre sus principales funciones las siguientes: a) Garantizar la seguridad de la información introducida y generada en los procesos que involucren recursos tecnológicos de la institución que administre la Dirección. B) Disponer las acciones que garanticen a consistencia, estandarización, confidencialidad y seguridad de la información/documentación que administra la Dirección. C) Administrar y monitorear la red local de equipos informáticos y telefónicos, ejecutando las medidas necesarias para mantenerla en funcionamiento continuo, eficiente y seguro. D) Dimensionar, planificar, desarrollar y administrar las bases de datos de la institución, disponiendo las medidas pertinentes para la estandarización, seguridad, respaldo, y recuperación de la información resguardada. E) Garantizar la administración y mantener activo el servicio del sistema de información comercial, así como suministrar oportunamente la información requerida por la Dirección Superior u otras dependencias autorizadas.

- La divulgación de la información solicitada, implica un alto riesgo, si en dado caso dicha información quiera utilizarse para realizar ataques físicos y/o digitales a los servidores donde se registra y resguarda la información de la ANDA y detener la operatividad en las agencias.
- Por ejemplo, los planes de contingencia no pueden ser divulgados por ser documentos de seguridad de la integridad de la información confidencial de ANDA, por los siguientes puntos: entre otros: a) Se detallan los procesos o pasos a seguir para la restauración de la información, se proporcionan nombres de bases de datos y servidores que contienen la información sensible. b) Se detallan los nombres completos del personal responsable por cada área, con sus datos personales y formas de localización, c) Se detallan las funciones y procedimientos designados para cada personal en el plan de contingencia, para recuperar la información sensible para la institución que le toca restaurar, proteger o validar.
- Divulgar los planes de contingencia o normas de seguridad de la ANDA a terceros, hacen vulnerable los planes de contingencia, la integridad de la información y la continuidad del negocio en ANDA. Lo anterior abre una puerta para que se pueda de alguna manera detener el funcionamiento de la institución, sistemas comerciales, servicios, etc.
- Por otra parte, la seguridad de la información, según las normas ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, como son los planes de contingencia, dentro de una organización.
- Asimismo, de acuerdo a la **certificación 98-367 Fundamentos de Seguridad de Microsoft**, se previenen ataques que afecten la seguridad física de los equipos del centro de datos, al ocultar la información de su ubicación y medidas de protección física, lógica y perimetral de los mismos.
- **Superficie de Ataque**
 Un concepto final que se debe enfrentar al evaluar la seguridad de nuestro entorno es el de una superficie de ataque. Con respecto a sistemas, redes y aplicaciones, ésta es otra idea que ha existido desde hace bastante tiempo. Una superficie de ataque consiste en un conjunto de métodos y vías que un atacante puede utilizar para penetrar a un sistema y, potencialmente, ocasionar daños. Entre mayor sea la superficie de ataque de un entorno en particular, mayor será el riesgo de un ataque exitoso.
- De la misma manera, al evaluar la superficie de ataque de la red, debemos tomar en consideración lo siguiente: a) Diseño general de la red, b) Colocación de los sistemas críticos.



Oficina de

uestra

- *La seguridad del sitio involucra la protección de las instalaciones físicas. Un concepto fundamental que se usa al diseñar un entorno de seguridad es el de la defensa a profundidad. La Defensa a profundidad significa la utilización de múltiples capas de seguridad para proteger sus activos. De esta manera, aún si un atacante viola una capa de defensa, cuenta con capas adicionales para mantener a esa persona fuera de las áreas críticas de su entorno.*
- *La seguridad informática consiste en los procesos, procedimientos, políticas y tecnología utilizados para proteger el sistema de informática.*
- *En relación a la información de la Distribución física de las sub unidades de la Dirección de Tecnología de Información, ésta es clave para calcular la superficie de ataque de un entorno, a menudo, la forma más sencilla es la de dividir la evaluación en tres componentes: a) Aplicación, b) Red y c) Empleado.*
- *Asimismo, en relación la información sobre el Listado de sistemas informáticos actualmente en producción y desarrollo, al evaluar la superficie de ataque de una aplicación, es necesario observar cosas tales como: a) La cantidad de código en una aplicación, b) el número de entradas de datos en una aplicación, c) el número de servicios en ejecución y d) Los puertos que la aplicación está escuchando.*

A partir del deber de motivación establecido en los artículos 65 y 72 LAIP, las resoluciones de los entes obligados deberán entregarse a la solicitante, a través del oficial de información mediante escrito con mención breve pero suficiente de sus fundamentos.

Con base a las facultades legales previamente señaladas y en vista que la solicitud cumple con todos los requisitos establecidos, en razón de lo antes expuesto y en lo estipulado en el Artículo 18 de la Constitución de la República de El Salvador, la suscrita Oficial de Información **RESUELVE: 1) CONCÉDASE EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA** dentro del plazo establecido por la LAIP, que se encuentra relacionada en romano II) de la presente resolución, incorporados en un folios que forma parte de la respuesta de lo solicitado. **2) HÁGALE SABER** al ciudadano, que lo peticionado en solicitud de información en los numerales 3, 5, 6, 7, 8 y 9, se encuentra clasificada bajo el índice de RESERVA en razón de lo manifestado en el romano III) de la presente resolución. **ENTRÉGASELE** a la solicitante la información requerida gestionada bajo el número de referencia **129-14-2018** por medio del presente informe oficial que consta de dos folios frente y vuelto que forman parte integral del informe. **3) NOTIFÍQUESE** la presente resolución y entréguese la información a la dirección electrónica proporcionada por el ciudadano como medio de comunicación y déjese constancia en el expediente respectivo.

Licda. Morena Guadalupe Juárez Guzmán
Oficial de Información Pública

Oficina de información y respuesta