ANEXO TÉCNICO No. 10 – GLOSARIO

ACCESS POINT: AP o WAP (Access Point o Wireless Access Point) También conocidos como puntos de acceso. Son dispositivos para establecer una conexión inalámbrica entre equipos y pueden formar una red inalámbrica externa (local o internet) con la que interconectar dispositivos móviles o tarjetas de red inalámbricas. Esta red inalámbrica se llama WLAN (Wireless local área Network) y se usan para reducir las conexiones cableadas.

ANS: Acuerdos de Niveles de Servicio - ANS, en inglés: Service Level Agreement -SLA, es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio**.**

ANSIBLE: Software que automatiza el aprovisionamiento de software, la gestión de configuraciones y el despliegue de aplicaciones. Está categorizado como una herramienta de orquestación, muy útil para los administradores de sistema y DevOps.

APPLIANCE: Son dispositivos de hardware dedicados (se encargan de realizar un número determinado de funciones), habitualmente diseñados para instalarse en un rack, que funcionan con software específicamente diseñado para ellos.

ATAQUE DOS: Un ataque de denegación del servicio -también conocido como ataque DoS (Denial-of-service attack).

APIS: Application Programming Interfaces, que en español significa interfaz de programación de aplicaciones.

BACKUP: La copia de seguridad de datos es un duplicado de los datos de un sistema de cómputo, que se toma y almacena en otro lugar, para poder usarse en caso de requerir restaurar el original después de un evento de pérdida de datos.

BACKBONE: Columna vertebral o una red troncal es aquella que conecta numerosos routers interconectados o pisos de la entidad.

BASTION HOST: Servidor bastion o pasarela de aplicaciones) es una aplicación que se localiza en un servidor con el fin de ofrecer seguridad a la red interna, por lo que ha sido especialmente configurado para la recepción de ataques, generalmente provee un solo servicio (como por ejemplo un servidor proxy).

BCP: Un plan de continuidad del negocio (o sus siglas en inglés BCP, por Business Continuity Plan) es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

BIA: El Business Impact Analysis permite a empresas estimar el impacto operacional y financiero de interrupciones.

BYPASS: Circuito que actúa como válvula modificando el flujo normal de datos hacia una ruta alternativa si se produce una caída de corriente o algún otro problema. Se utiliza en sistemas de alta disponibilidad.

BYOD: Bring Your Own Device, en español trae tu propio dispositivo, se define como la práctica en la que se alienta a los trabajadores al uso de los dispositivos propios para acceder a los sistemas y datos empresariales.

BREAKERS: Interruptor de circuito) tiene como función principal proveer protección a equipos eléctricos y cableado.

CENTRO ALTERNO DE OPERACIÓN (CAO): es el lugar en el cual los colaboradores de ENTerritorio pueden reanudar las operaciones del día a día, ante la afectación de sus oficinas principales por eventos contingentes. Este estará retirado del centro de operación normal.

CENTRO DE CÓMPUTO ALTERNO (CCA): es el lugar de procesamiento y almacenamiento de información que soporta la operación tecnológica de la Entidad en caso de presentarse una contingencia.

CENTRO DE CÓMPUTO ALTERNO (CCA): es el lugar de procesamiento y almacenamiento de información que soporta la operación tecnológica de la Entidad en caso de presentarse una contingencia.

CENTRO DE CÓMPUTO BÁSICO EDIFICIO ENTERRITORIO (CCB): es el lugar de procesamiento y almacenamiento de información que soporta la operación tecnológica básica de la Entidad.

CENTRO DE CÓMPUTO PRINCIPAL (CCP): es el lugar de procesamiento y almacenamiento de información que soporta la operación tecnológica normal de la Entidad.

CERTIFICADO DIGITAL WILDCARD: Es un certificado de clave pública que se puede utilizar con varios subdominios de un dominio.

CLÚSTER: Conjuntos o conglomerados de dispositivos construidos mediante la utilización de hardware comunes y que se comportan como si fuesen una única computadora.

CMBD: (Configuration Management DataBase) es un concepto que introduce ITIL – ISO 20000 para facilitar la gestión de los servicios TI. Se define como una base de datos donde administrar y gestionar todos los elementos de la compañía (Configuration Items ó CI) que son necesarios para la prestación de servicios. En esta última frase hay que resaltar la palabra todos, porque se introducirán, no solamente los elementos TIC (servidores, firewall, routers), sino que se tendrán que introducir también los servicios de proveedores, el software, las personas, documentación, etc.

COBIT (Control Objectives for Information and Related Technology): Provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

CORE: El término Switch troncal se refiere a los que se utilizan en el núcleo central (core) de las grandes redes.

CROSS CONECTION: Esquema de conexión entre corridas de cableado, subsistemas y equipo por medio de cordones de parcheo o puentes que se conectan al hardware de conexión en cada extremo.

DNS: Sistema de nombres de dominio.

DISPONIBILIDAD: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

DLP (Data Loss Prevention): Es un sistema que está diseñado para detectar potenciales brechas de datos/ transmisiones de datos y prevenirlos a través de monitoreo, detección y bloqueo de información sensible mientras está en uso, en movimiento y en reposo.

DRP: (Disaster Recovery Plan), es un sistema con el cual las organizaciones se preparan contra posibles desastres de diversos indoles.

DUAL STACK: En esta red, operan de forma simultánea IPv4 e IPv6. En una red dual stack, ambos protocolos son desplegados completamente y los protocolos de enrutamiento deben llevar los prefijos correspondientes a cada tecnología, de manera transparente. La mayor desventaja de esta aproximación ideal es que requiere que todo el equipamiento soporte ambos protocolos, lo cual no es la situación real.

ECC: Error Correcting Code", que implica que la memoria RAM tiene un bit extra, el cual representa un código programado para detectar errores en el procesador.

EMT: (Electrical Metallic Tubing). De pared delgada o liviana, ofrece protección mecánica a conductores eléctricos.

END POINT: Dispositivo informático remoto que se comunica con una red a la que está conectado.

EOL (End Of Life): término usado en la informática para designar el fin del ciclo de vida (signifique esto soporte o ventas) del producto.

ETHERNET: Tecnología que conecta redes de área local (LAN) cableadas y permite que el dispositivo se comunique entre sí a través de un protocolo que es el lenguaje de red común.

FASTETHERNET: Ethernet de alta velocidad es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps (megabits por segundo).

GATEWAY AUDIOCODE: Los Gateways o pasarelas IP se utilizan para combinar las líneas de teléfono analógicas o digitales con sistemas telefónicos 100% basados en IP, o bien para utilizar servicios IP sobre una central analógica o digital tradicional. Su función es convertir la voz tradicional en datos IP y viceversa.

GIGABITETHERNET: Versión de la tecnología Ethernet ampliamente utilizada en redes de área local (LAN) para transmitir tramas o frames Ethernet a 1 Gbps.

Gb: Unidad de medida Giga Byte.

Ghz: Unidad de medida Giga Hertz.

GUSANO: Un gusano informático es un tipo de programa de software malicioso cuya función principal es infectar otras computadoras mientras permanece activo en los sistemas infectados.

HA: Siglas en ingles de alta disponibilidad.

HARDENING: (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo.

HASH: Una función criptográfica hash- usualmente conocida como "hash"- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

IDS: (Intrusion Prevention System) o sistema de prevención de intrusiones: es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva.

IAAS: El concepto de Infraestructura como Servicio, en inglés: Infrastructure as a Service – IaaS, es uno de los tres modelos fundamentales en el campo del cloud computing, junto con el de Plataforma como Servicio,

en inglés: Platform as a Service – PaaS y el de Software como Servicio, en inglés: Software as a Service – SaaS.

INFORMACIÓN: Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y completitud de la información y asegurar que sus métodos de procesamiento sean exactos.

IPV4: El Protocolo de Internet versión 4, en inglés: Internet Protocol Versión 4 –Ipv4, es la cuarta versión del Internet Protocol (IP).

IPV6: El Protocolo de Internet versión 6, en inglés: Internet Protocol Versión 6 – Ipv6, es una versión del Internet Protocol – IP, diseñada para reemplazar a Internet Protocol Versión 4 – Ipv4, que se está implementado en la gran mayoría de dispositivos que acceden a Internet.

ISP: Proveedor de Servicios de Internet (Del inglés Internet Service Provider), es el término con el que se identifica a las compañías que proporcionan acceso a Internet.

ITIL: es un acrónimo de Biblioteca de Infraestructura de Tecnologías de la Información (por sus siglas en inglés, Information Technology Infrastructure Library). Es un conjunto de publicaciones de mejores prácticas para Gestión de servicios de TI. ITIL proporciona asesoramiento sobre la provisión de servicios de TI de calidad y de los procesos, funciones y demás capacidades necesarias para darles apoyo. El marco de ITIL está basado en un ciclo de vida del servicio y consiste de cinco etapas (estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio) que cuentan con su propia publicación de apoyo.

ISO27001: Esta norma es un estándar para la seguridad de la información emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

FIREWALL: También llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso. Permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red.

LAN: Siglas en ingles de Local Area Network, aplicado a las redes cableadas que conecta uno o más dispositivos dentro de un ámbito pequeño y limitado.

LÍNEA BASE: Valor del indicador que se establece como punto de partida para evaluarlo y darle seguimiento.

LOG: es un archivo que registra los eventos que ocurren en un sistema de cómputo, dispositivo de red o terminal de usuario.

MALWARE: Programa malicioso, software dañino o software malintencionado que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Mbps: Unidad de medida Megabyte por Segundo.

MPLS: La conmutación de etiquetas multiprotocolo o **MPLS** (del inglés Multiprotocol Label Switching) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI.

NAC: Es el conjunto de tecnologías cuyo objetivo es hacer cumplir a todos los dispositivos que forman parte de una red las políticas de seguridad informática que se hayan establecido dentro de una organización y que así en el caso de que se diera alguna situación de ataque o de fraude, aportará las mejores soluciones para que nuestro sistema vuelva a ser infranqueable. Lo que hace este control de acceso a red es limitar la introducción de los usuarios y dispositivos dentro de la red, pudiendo así solo entrar aquellos que cuenten con la autenticación adecuada.

NETWORKING: Integración de dos sistemas de redes completas. Una red consiste en dos o más computadoras unidas que comparten recursos como archivos, CD-Roms o impresoras, y que son capaces de realizar comunicaciones electrónicas. Las redes están unidas por cable, líneas de teléfono, ondas de radio, satélite, etc.

NETWORK ASSESTMENT: El Assessment de red permite la rápida identificación del equipo que está acarreando algún incidente, además, proporciona una reducción de tiempo muy grande en ese proceso en relación a las empresas que necesitan hacer una exploración para descubrir dónde está el equipo con problema.

NOC: Siglas en Ingles de Network Operation Center, asociado al centro de monitoreo.

NUBE: La computación en la nube, conocida también como servicios en la nube, informática en la nube, nube de cómputo o nube de conceptos (del inglés cloud computing), es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

NUBE AWS: Azure es una nube pública de pago por uso que te permite compilar, implementar y administrar aplicaciones en una red global de Datacenter (centros de datos) de Amazon Web Services.

NUBE AZURE: Azure es una nube pública de pago por uso que te permite compilar, implementar y administrar aplicaciones en una red global de Datacenter (centros de datos) de Microsoft.

OVM: Solución de virtualización, compuesta de Oracle VM Server y Oracle VM Manager, que permite implementar sistemas operativos y aplicaciones empresariales dentro de un entorno de virtualización totalmente compatible.

PATCH CORD: Cable de Conexión se le llama al cable (UTP, F.O., etc.) que se usa en una red para conectar un dispositivo electrónico con otro

PARCHE: Un parche es un conjunto de cambios en un software o firmware, o en sus datos de apoyo, diseñados para actualizarlo, corregirlo o mejorarlo. Esto incluye corregir vulnerabilidades de seguridad y otros errores. Los parches a menudo se escriben para mejorar la funcionalidad, usabilidad o rendimiento de un programa.

PBX: “Private Branch Exchange”, la cual es una red telefónica privada utilizada dentro de una empresa.

PENTESTING: Ciberataque simulado contra su sistema informático para verificar y analizar vulnerabilidades explotables. En el contexto de la seguridad de aplicaciones web, las pruebas de penetración de seguridad informática se usan para detectar, mitigar y frustrar ataques avanzados.

PHISING: Técnica de ciberdelincuencia que utiliza el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información personal confidencial.

POOL DE DIRECCIONES: Conjunto de recursos de direcciones IP inicializados que se mantienen listos para su uso, en lugar de ser asignados y destruidos bajo demanda.

PROOF TEST (Método de ensayo): Prueba de presión hidrostática estándar de hoy en día intenta verificar tanto la capacidad de presión como la hermeticidad de las juntas de una tubería.

PSTN: Red Telefónica Pública Conmutada, las llamadas locales y de larga distancia son posibles gracias a ella. Se trata de una red telefónica clásica en donde se da una comunicación de voz en tiempo real, asegurando fluidez en el tráfico de la red.

RAM (MB): Random Access Memory (memoria de acceso aleatorio) es un componente que forma parte del ecosistema de hardware y que tiene como mayor finalidad crear un puente entre el sistema operativo, software, procesador y otros dispositivos para que estos intercambien información entre ellos.

RANSOMWARE: es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción

RFCs: Los Request for Comments, más conocidos por sus siglas RFC, son una serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos.

ROLLBACK: Rollback o reversión o flagare es una operación que devuelve a la base de datos a algún estado previo.

RPO: El Recovery Point Objective es la cantidad de datos que una empresa puede permitirse perder y aun así seguir funcionando si sufre un tiempo de inactividad (“downtime”).

RTO: Recovery Time Objective Tiempo que lleva solucionar el incidente antes de que todos los sistemas se reanuden con normalidad.

RSA: Algoritmo criptográfico de clave pública. El RSA funciona basándose en una clave pública y privada.

SIP: “Session Initiation Protocol”, es un protocolo de señalización de telefonía IP utilizado para establecer, modificar y terminar llamadas VOIP.

SOC: Security Operations Center (SOC) es un servicio de ciberseguridad para la infraestructura TI de las empresas en modalidad 7/24. Protege, detecta y responde frente a amenazas de seguridad que afecten al negocio y los incidentes que estas puedan causar.

SDK: Kit de desarrollo de software (SDK), un conjunto de herramientas que ofrece generalmente el fabricante de una plataforma de hardware, un sistema operativo (SO) o un lenguaje de programación. Los SDK permiten que los desarrolladores creen aplicaciones específicas para la plataforma, el sistema o el lenguaje de programación.

SERVICIOS DE NUBE (TENANTS): Es el modelo de despliegue de Computación en la Nube de uso exclusivo en donde la infraestructura es operada únicamente para una organización. Puede ser administrada por la organización o por un tercero y puede existir tanto en las instalaciones del primero como fuera de ellas.

SIEM: Gestión de Eventos e Información de Seguridad (Security Information and Event Management) es un sistema de gestión de información y eventos de seguridad, centralizando el almacenamiento y la interpretación de los datos relevante de seguridad.

SPOC: El término Single Point of Contact o SPOC se utiliza a nivel técnico para referirse al punto central de contacto para mantener la comunicación con clientes y usuarios.

SOC: Siglas en inglés de Security Operation Center, asociado al Centro de Monitorio de Seguridad.

SPYWARE: El programa espía es un programa maligno que recopila información de una computadora y después transmite esta información a una Entidad externa sin el conocimiento o el consentimiento del propietario del computador.

SSO: Inicio de Sesión Único o Inicio de Sesión Unificado.

STREAMING: Es un tipo de tecnología multimedia que envía contenidos de vídeo y audio a un dispositivo conectado a Internet. Esto le permite acceder a contenidos (TV, películas, música, pódcast) en cualquier momento que lo desee, en un PC o un móvil.

STREAMYARD: Es una herramienta o programa digital para realizar transmisiones de vídeo en Streaming por redes sociales, con la característica de acceso desde el navegador.

STORAGE: Almacenamiento de información.

SWITCHES: Switch perimetral se refiere a los utilizados en el nivel jerárquico inferior en una red local y a los que están conectados los equipos de los usuarios finales.

SWITCHES CORE: El término Switch troncal se refiere a los que se utilizan en el núcleo central (core) de las grandes redes. Es decir, a estos switches están conectados otros de jerarquía inferior, además de servidores, routers WAN.

TB: Terabyte es el término dado a 1.000 gigabytes, por lo que se convierte en el siguiente término "byte" después del gigabyte.

TENANT: Grupo de usuarios que comparten un acceso común con privilegios específicos a la instancia de software, separando los datos sensibles

TENGIGABITETHERNET IEEE 802.3ae: Define una versión de Ethernet con una velocidad nominal de 10 Gbit/s, diez veces más rápido que gigabit Ethernet.

TERRAFORM: Tecnología de Infrastructure as Code (IAC) que nos permite definir, entre otras cosas, los recursos en la nube que vamos a aprovisionar para el despliegue de nuestras aplicaciones.

TIA/EIA-568-B: Especifica un sistema de cableado para edificios comerciales, con soporte multiproducto y multimarca también provee información para el diseño de productos de telecomunicaciones por parte de los fabricantes.

TIC: Son las Tecnologías de la información y la comunicación que agrupan los elementos (hardware, software, firmware) y las técnicas utilizadas en el tratamiento y la transmisión de información.

TIC: Son las Tecnologías de la información y la comunicación que agrupan los elementos (hardware, software, firmware) y las técnicas utilizadas en el tratamiento y la transmisión de información.

TROYANO: Es un programa maligno que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

TROUGHTPUT: Tasa real de que la información es transferida.

TOGAF (The Open Group Architecture Framework): Es una de las metodologías más populares para desarrollar AE. Es una herramienta para asistir en la aceptación, creación, uso, y mantenimiento de arquitecturas. Está basado en un modelo iterativo de procesos apoyado por las mejores prácticas y un conjunto reutilizable de activos arquitectónicos existentes

UAT (User Acceptance Tolerance): La prueba de aceptación del usuario verifica si un software está cumpliendo los objetivos iniciales de acuerdo con los requisitos del usuario.

VCPU: Unidad de medida de procesamiento en núcleos o Cores.

VLAN: Una red de área local virtual (Virtual Local Area Network o VLAN) es un segmento lógico más pequeño dentro de una gran red física cableada.

VPN SITE-TO-SITE: Una red privada virtual es una tecnología de red de ordenadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

WAF: Web Application Firewall (WAF) protege de múltiples ataques al servidor de aplicaciones web en el BackEnd. La función del WAF es garantizar la seguridad del servidor web mediante el análisis de paquetes de petición HTTP / HTTPS y modelos de tráfico.

WAKE ON LAN: Wake on LAN (WoL) es un protocolo que permite encender de forma remota tu ordenador cuando este esté apagado, suspendido o hibernando.

WAN: Siglas en ingles de Wide Area Network, aplicado a las redes de gran tamaño, generalmente dispersa en un área metropolitana, a lo largo de un país o incluso a nivel mundial.

WEB: World Wide Web (también conocido como «la Web»), sistema de documentos (o páginas web) interconectados por enlaces de hipertexto, disponibles en Internet.

WIPE: En un ámbito informático, Wipe hace referencia a borrar una partición o "limpiar" una partición.

WLAN: Siglas en ingles de Wireless Local Area Network, de una red de área local que conecta equipos sin necesidad de cables.

TI: tecnología de la información (TI) El término es utilizado como sinónimo para los computadores, y las redes de computadoras, pero también abarca otras tecnologías de distribución de información, tales como la televisión y los teléfonos. Múltiples industrias están asociadas con las tecnologías de la información, incluyendo hardware y software de computador, electrónica, semiconductores, internet, equipos de telecomunicación, e-commerce y servicios computacionales. En estos documentos TI se identifica como el grupo de tecnologías de la información que acompaña la entidad en todos los requerimientos asociados a las tecnologías de información, redes, hardware y software.

TIA/EIA-568: Set de estándares desarrollado por la Telecommunications Industry Association referido al cableado comercial para productos y servicios de telecomunicaciones.

VIP: Vip o VIP es una expresión que se emplea en diversos ámbitos para designar a personajes importantes que requieren una atención especial.