Bogotá D.C, martes 18 de agosto de 2020

PARA: CATALINA VALENCIA TOBÓN
Dirección General

DE: CARLOS ALBERTO QUITIAN SALAZAR
Área de Control Interno

ASUNTO: Informe continuidad del negocio en el marco de emergencia COVID-19

Cordial saludo Catalina,

En desarrollo de la versión 3 del Plan Anual de Auditoría del Idartes para la vigencia 2020 y en cumplimiento a las disposiciones establecidas por la Circular Externa 100-10 de 2020 Vicepresidente de la República - Departamento Administrativo de la Función Pública en su numeral 5. *Hacer seguimiento a los planes de acción que comienzan a surgir como contingencia, verificando el cumplimiento de normas que se han proferido a partir de la declaratoria de la emergencia sanitaria a causa del COVID-19, tanto nacionales como locales* (Laborales, tributarias, de salud, de atención ciudadana, entre otras), de manera atenta anexo a esta comunicación el informe de continuidad del negocio en tiempos de la emergencia COVID-19

Es necesario de acuerdo con las recomendaciones documentadas en el informe, dar prioridad a la construcción, adopción y divulgación del Plan de Continuidad de Negocio siendo este un requisito del manual de Gobierno Digital adoptado mediante el Decreto 1078 de 2015.

Por otra parte, también se recomienda dar prioridad a la a la actualización de los siguientes documentos institucionales:

- Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información
- Plan de Seguridad y Privacidad de la Información
- Política de seguridad de la información

El informe referido fue comunicado a la Subdirección Administrativa y Financiera.

Cordialmente,

CARLOS ALBERTO QUITIÁN SALAZAR
Asesor de Control Interno
Documento firmado electrónicamente por:

CARLOS ALBERTO QUITIAN SALAZAR, Asesor Control Interno, Área de Control Interno,
Fecha firma: 19-08-2020 10:39:21

34b7fb40cbd5bd0dd0f58005d843ad50d49d01f6ad77c2abad63a29578c6eed2

INFORME DE SEGUIMIENTO NORMATIVIDAD COVID-19
CONTINUIDAD DE NEGOCIO

PRIMER INFORME

ÁREA DE CONTROL INTERNO

INSTITUTO DISTRITAL DE LAS ARTES

BOGOTÁ D.C.
AGOSTO DE 2020

Instituto Distrital de las Artes - Idartes
Carrera 8 No. 15-46, Bogotá, D.C. Colombia
Teléfono: 3795750
www.idartes.gov.co
e-Mail: contactenos@idartes.gov.co

Tabla de contenido

INTRODUCCIÓN

En desarrollo del Plan Operativo Anual de Idartes para la vigencia 2020 versión 2 y en cumplimiento a las disposiciones establecidas Circular Externa 100-10 de 2020 Vicepresidente de la República - Departamento Administrativo de la Función Pública en su numeral *5. Hacer seguimiento a los planes de acción que comienzan a surgir como contingencia, verificando el cumplimiento de normas que se han proferido a partir de la declaratoria de la emergencia sanitaria a causa del COVID-19, tanto nacionales como locales (Laborales, tributarias, de salud, de atención ciudadana, entre otras).*

Para el Instituto Distrital de las Artes, se procede a realizar el seguimiento del cumplimiento relacionado con la normatividad COVID-19 para lo corrido del segundo trimestre de 2020 relacionado con en materia de la continuidad de negocio.

1. OBJETIVO

Realizar seguimiento al cumplimiento de las normas relacionadas con el COVID-19 implementadas en la gestión del Instituto Distrital de la Artes – Idartes, en materia de continuidad de negocio.

2. MARCO NORMATIVO

- Ley 1437 de 2011, art 61
- Decreto 1008 de 2018, Capitulo 1
- Circular 047 de 2020
- Política de Gobierno Digital
- Guía de Lineamientos para documentos electrónicos

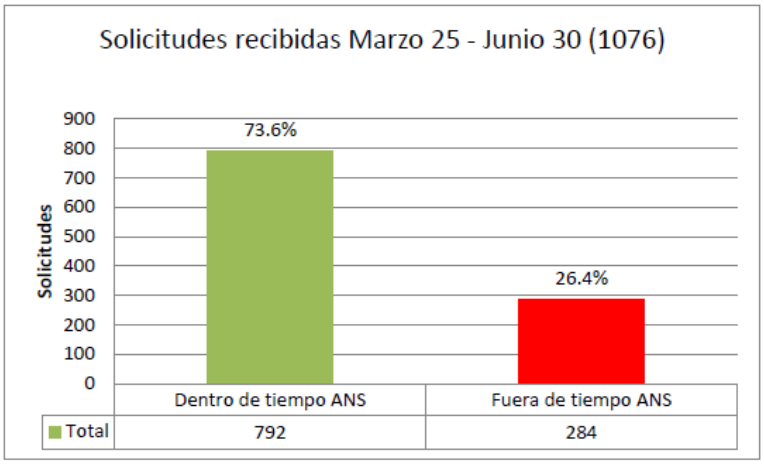
3. CRITERIOS DE EVALUACIÓN

Para el presente informe, es el resultado de la verificación de la normatividad referente a la continuidad de negocio, seguridad de la información en el marco de la actual situación a causa del COVID 19, se verifica la información aportada tal como lo es, Información estadística de prestación de servicios de soporte, así como las tipologías de soporte gestionados, las soluciones de seguridad y en qué tipo de información se enfoca, actividades de cumplimiento de la Política de Seguridad de la Información, actualización del mapa de riesgos y sus respectivos controles, cumplimiento de los lineamientos para el uso de documentos electrónicos, construcción de la sede electrónica, actividades en el marco de la emergencia debido al COVID 19 y evidencias de construcción del Plan de Continuidad de Negocio PCN, a continuación se analiza la información aportada.

4. RESULTADOS DE LA EVALUACIÓN

4.1. PRESTACIÓN DE SERVICIOS DE SOPORTE (DESDE 25/03/2020 HASTA 30-06/2020)

De acuerdo con la información aportada por el Área de Tecnología, se presentaron un total de 1076 solicitudes en la plataforma de mesa de ayuda, de las cuales **792** equivalente al **73,6%** se cumplieron dentro del tiempo establecido en los Acuerdos de Niveles de Servicio ANS y **284** equivalente al **26,4%** atendidas fuera de tiempo, como se evidencia en la gráfica del anexo "INFORME MESA DE AYUDA GLPI"



Grafica 1 Tiempos de servicio ANS de las solicitudes recibidas

En la información aportada a través del radicado 20204000196373, se hace referencia exclusivamente a las 792 solicitudes gestionadas dentro del tiempo ANS, lo cual genera un sesgo en el análisis proporcionado por el área de tecnología. Adicionalmente no se analiza el porqué de la gestión de dichas solicitudes fuera del tiempo ANS.

Con referencia a las categorías de soporte, se evidencia que la mayor necesidad de soporte durante el periodo analizado en condiciones de aislamiento y de trabajo en casa, ha presentado el siguiente comportamiento:

La mayor concentración de necesidades de soporte son las categorías de:

- La plataforma Si Capital y otras
- Cuentas de Acceso - Correo electrónico
- Conectividad vía VPN
- Cuentas de acceso – Perfil de usuario

Siendo con 526 solicitudes el **50%** del top de las categorías tal como se muestra a continuación:

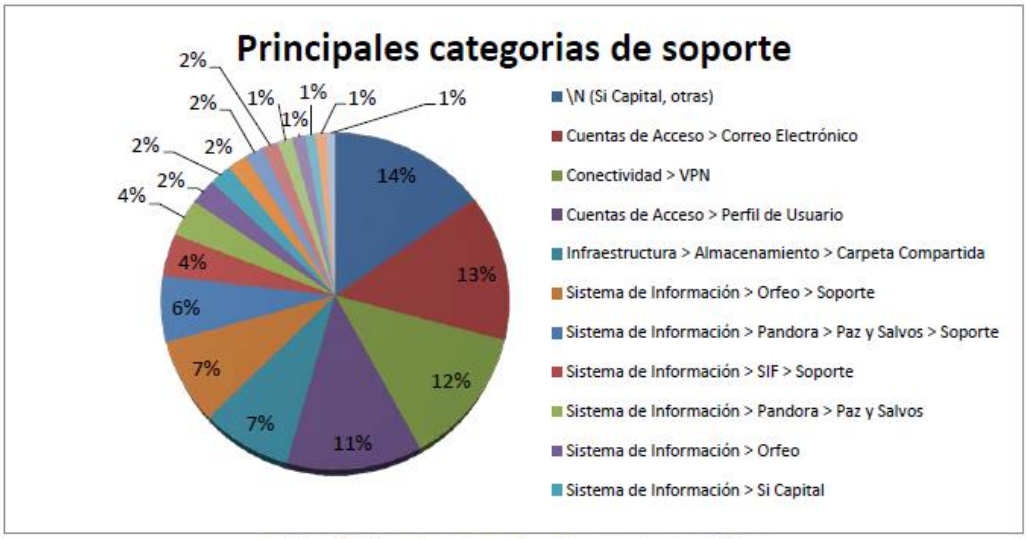


Gráfico 3: Top de categorías de soportes recibidas

Tal como es analizado por el área de tecnología se viene presentando un incremento en las categorías de conectividad VPN, infraestructura – Almacenamiento – Carpeta compartida, el Sistema de Gestión Documental Orfeo junto con el soporte a otros sistemas de información tales como los son Pandora y SIF, debido a que son sistemas que se han implementado para apoyar la gestión virtual de actividades.

4.2. TIPOS DE SOLICITUDES

El 94.8% de las solitudes recibidas corresponden a incidencias no previstas y el 5.2% corresponde a requerimientos como se evidencia a continuación:

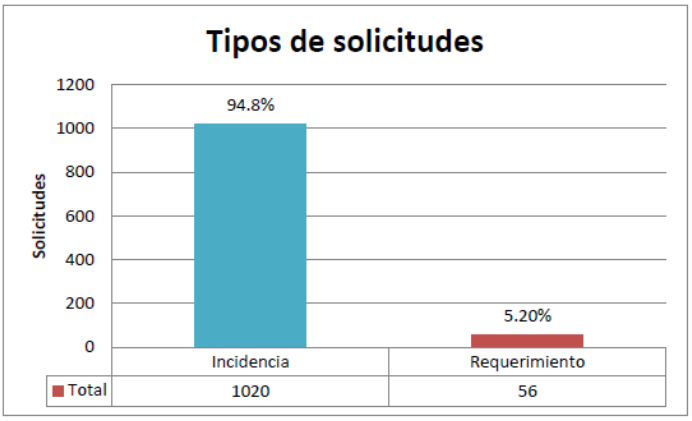


Gráfico 4: Tipos de Solicitudes

4.3. CANALES DE RECEPCIÓN DE SOLICITUDES

A través de correo electrónico se recibieron 1053 solicitudes equivalente al 98% y 23 de las solicitudes equivalentes al 2% fueron generadas a través de Helpdesk (Mesa de ayuda) tal como se muestra a continuación:

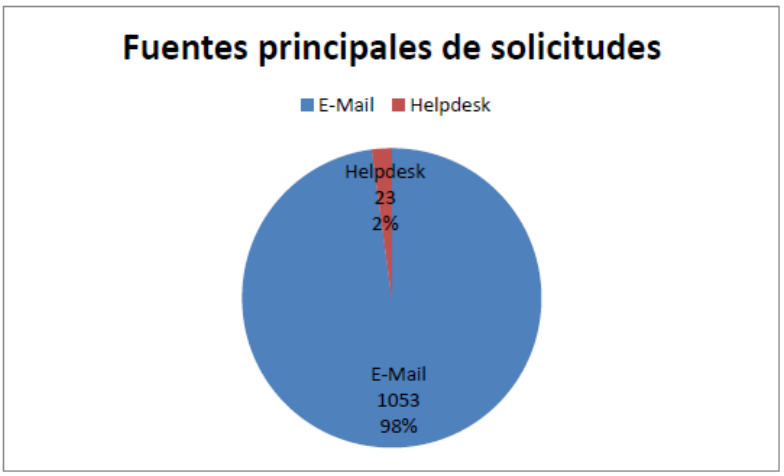


Gráfico 5: Medios de recepción de solicitudes

4.4. SOLUCIONES DE SEGURIDAD

Idartes cuenta con un sistema de seguridad perimetral para proteger sus sistemas de información, herramientas, aplicaciones, red de voz y datos, el cual está compuesto por:

- Licenciamiento y consola de Anti-virus KASPERSKY: enfocada en brindar seguridad para los PC y servidores de la Entidad, por medio de escaneo de antivirus para software y archivos, monitorización de actividad, búsqueda de vulnerabilidades y control de tráfico en Internet.

- FIREWALL – FORTINET y PfSense: enfocado a brindar prevención de intrusos y filtrado web, monitorear el tráfico de red - entrante y saliente, control de aplicaciones, protección total de contenidos, conexiones virtuales privadas y seguras – VPN, basado en un conjunto definido de reglas de seguridad.

- Servicio Controlador de Dominio: enfocado en garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, basado en un conjunto definido de reglas de acceso lógico (roles, permisos) y grupos se seguridad.

- Circuito cerrado de Televisión – CCTV: enfocado a la seguridad y el control de acceso físico a las diferentes áreas, escenarios y sedes de la Entidad, permite prevenir, detectar, anunciar, reaccionar y suministrar evidencia grabada ante una situación.

4.5. CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

4.5.1. MONITORES DE RED

La entidad cuenta con las aplicaciones mencionadas en el numeral anterior. Adicionalmente, la entidad cuenta con una herramienta libre llamada ZABBIX para

monitorear los servicios de red hardware (servidores, equipos, switchs y software), y certificados SSL para garantizar conexiones seguras en los sistemas de información WEB y autenticidad en los portales institucionales.

4.5.2. SOFTWARE PARA COPIAS DE RESPALDO

IDARTES cuenta actualmente con la solución Veritas Backup Exec para la elaboración de copias de respaldo de los sistemas misionales, de apoyo, herramientas, aplicaciones e información alojada en los equipos especializados para almacenamiento de información SAN y NAS.

La solución Veritas Backup Exec se encuentra instalada y configurada en el Data Center de la sede principal, de manera tal que realice copias de seguridad de manera incremental o total conforme sea el caso requerido. Se realizan copias de los sistemas y bases de datos de KOHA, SIF, ORFEO SICAPITAL, PANDORA, CREA y PHPLIST.

No obstante, en el caso de los sistemas con motor de base de datos Oracle como SI Capital, se cuenta con un respaldo en la sede Planetario donde el VCenter, cuenta con una réplica del servidor de SI Capital principal y realiza el movimiento de las copias de seguridad mediante la VPN IPSec entre sede principal y el escenario.

Por otra parte, el sistema de información SIF, portales institucionales y sitio WEB, en el marco del contrato interadministrativo ETB – Hosting, contamos con el servicio de copias de respaldo generadas y administradas por las áreas, quienes administran dichos equipos.

4.5.3. ACTIVIDADES DE SALVAGUARDA

Las actividades que la entidad viene realizando con la finalidad de salvaguarda de la información son:

- Implementación del modelo de seguridad y privacidad de la información.
- Revisión e implementación de controles físicos y administrativos.
- Jornadas de sensibilización y capacitaciones a los usuarios en Seguridad de la Información.
- Alistamiento del material para sensibilización y capacitación en seguridad de la información.
- Mesas de trabajo para la revisión de políticas de seguridad con la Oficina Asesora Jurídica, SAF-Gestión Documental y SAF-Tecnología.
- Depuración y estandarización de credenciales de acceso en el controlador de dominio, sistemas de información y correo institucional, para brindar acceso según rol a servicios de red, carpetas compartidas y sistemas de información.
- Copias de respaldo aplicaciones y bases de datos.
- Conexiones seguras a información institucional por medio de VPN.
- Replicación de bases de datos sistemas de apoyo en centro alterno – Planetario.

- Desarrollo de sistemas de información aplicando las buenas prácticas, políticas de control de acceso y de seguridad de la información.
- Actualización y elaboración de procedimientos de Seguridad y Privacidad de la Información.
- Gestión del riesgo y verificación del cumplimiento de controles y políticas establecidos.

4.5.4. SEGURIDAD Y COPIA DE RESPALDO DE ORFEO

Apoyado por la solución Veritas Backup Exec se efectúan copias de seguridad tal como se menciona en el numeral 6.2. Adicionalmente de la realización de copias de respaldo al Sistema de Gestión Documental ORFEO también se realiza a su base de datos, almacenas en la data Center sede principal y del mismo modo se cuenta con un certificado SSL que brinda seguridad y autenticidad al subdominio.

4.6. RIESGOS Y CONTROLES IDENTIFICADOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA MODALIDAD DE TRABAJO EN CASA.

Pese a que se menciona la realización de actividades para garantizar la seguridad y privacidad de la información antes relacionadas, también incluidas en el INFORME DE AVANCES SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD IDARTES con corte junio 30 2020, no se evidencia la formulación y control de riesgos relacionados con la modalidad de trabajo en casa.

4.7. CON REFERENCIA A LA GUÍA DE LINEAMIENTOS PARA EL USO DE DOCUMENTOS ELECTRÓNICOS

4.7.1. IMPLEMENTACIÓN DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO Y MEDIDAS COMPLEMENTARIAS TALES COMO FIRMAS DIGITALES, MECANISMOS DE ENCRIPTACIÓN Y HABILITACIÓN DE FUNCIONES DE ENVÍO Y LECTURA.

Entre las últimas mejoras e implementaciones que están relacionadas con documento electrónico están:

- Implementación Fase 1 de firma electrónica interna y de salida (inició el 4 de mayo de 2020).
- Radicación y firma electrónica de solicitudes de pago de contratistas.

4.8. SEDE ELECTRÓNICA IDARTES O ATENCIÓN POR OTROS CANALES

En el marco de lo que se denomina sede electrónica, desde el año 2019 y el primer semestre del 2020, a través del trabajo articulado con las diferentes dependencias de la entidad, la Alta Consejería Distrital de TIC y Área de Administración Funcional

Bogotá te escucha – Secretaría General se realizó el paso a producción y avance en interoperabilidad de los trámites:

- Bogotá te escucha
- Comisión Fílmica
- Préstamo de escenarios

Para éste siguiente semestre se trabajará en:

- Módulo para que los ciudadanos puedan verificar el estado de su trámite en línea.
- Módulo para comprobación de validez de documentos firmados electrónicamente por la entidad y enviados a ciudadanos, empresas u otras entidades públicas. Esto como parte de la fase 2 de la firma electrónica.
- Uso y apropiación del mecanismo de firma electrónica y trámites.
- Certificación de la entidad en interoperabilidad nivel 2 MINTIC.
- Registro y actualización de los tramites mencionados en el portal del estado colombiano www.gov.co.

4.9. LINEAMIENTOS DE POLÍTICA DE GOBIERNO DIGITAL Y LEY 1437 DE 2011

En el marco de la Política de Gobierno Digital y el artículo 61 de la ley 1437 de 2011 la entidad ha dispuesto las siguientes cuentas de correo:

- Recepción de radicaciones: gestión.documental@idartes.gov.co
- Atención al ciudadano: contactenos@idartes.gov.co
- Notificaciones judiciales: notificacionesjudiciales@idartes.gov.co

4.10. ACTIVIDADES EN EL MARCO DE LA EMERGENCIA SANITARIA POR COVID 19

La Subdirección Administrativa y Financiera desde el inicio de la emergencia sanitaria, en articulación con las demás Subdirecciones, Oficinas y Dependencias, a través de los diferentes canales de comunicaciones institucionales y jornadas de capacitación, dio a conocer y promovió el uso y apropiación de herramientas, tecnologías, instructivos, sistemas de información web, video tutoriales, entre otros, con el fin de garantizar el trabajo desde casa, trámites y radicación de correspondencia.

También se cuenta con el servicio de correo certificado para el envío de comunicaciones a través del contrato No. 1311-2019 con REDEX S.AS. 1311- 2019.

4.11. PLAN DE CONTINUIDAD DE NEGOCIO

4.11.1. ACTIVIDADES ENFOCADAS EN MANTENER LA CONTINUIDAD DE LA PRESTACIÓN DE LOS SERVICIOS INSTITUCIONALES

En el marco de los diferentes contratos de prestación de servicios, soporte renovación de licenciamiento y convenios interadministrativos suscritos con la ETB conectividad y hosting, se han adquirido y renovado servicios con el fin de soportar la continuidad del negocio y la operación, así como garantizar la prestación de los servicios tecnológicos de red, sistemas de información, herramientas y aplicaciones, tales como:

- Almacenamiento en la nube
- Servicio de back up de información y bases de datos críticas
- Conectividad
- Soporte licenciamiento base de datos
- Servicios plataforma G-SUITE (Google)
- Renovación licenciamiento y soporte sistema de seguridad perimetral

Así mismo, se incluyeron proyectos en el PETI, para el fortalecimiento Institucional de la infraestructura tecnológica (hardware-software) que garanticen la prestación de servicios institucionales eficientes y de calidad.

4.12. DOCUMENTO PLAN DE CONTINUIDAD DE NEGOCIO

En el marco del Plan de Implementación del Modelo de Seguridad y Privacidad de la Información, se incluyeron actividades para actualizar el plan de contingencia y continuidad de la operación de tecnologías de la información, el cual se encuentra en fase de análisis y planeación con referencia a los siguientes criterios:

- Determinar la infraestructura critica actual que debe ser respaldada ante cualquier emergencia y desastre. Así como, la infraestructura Hardware Software mínima requerida para la operación de la entidad.
- Actualizar y divulgar la política de seguridad y continuidad de la operación.
- Fortalecer los controles administrativos, físicos, lógicos y medidas preventivas.
- Realizar simulacro para establecer las actividades y tiempos de respuesta y recuperación ante desastres.

A pesar que se menciona en la información aportada a través del radicado 20204000196373 en las páginas 6 y 7, la elaboración de un instrumento técnico como herramienta base para la construcción del PCN (Plan de Continuidad de Negocio), el cual establece las líneas de acción con las que se dará respuesta a los procesos críticos y a los riesgos asociados en las etapas preventiva, reactiva y de restablecimiento de conformidad con la metodología establecida por el DAFP, el Área de Control Interno en el momento de la verificación, no encontró evidencias de su fase de construcción por lo cual se requiere que se adelanten las actividades pertinentes debido a que lo expuesto incumple lo establecido en el Decreto 1008 de

2018 Artículo 2.2.9.1.1.3. “Principio de Seguridad de la Información” y lo determinado por el Manual de Gobierno Digital el cual establece en la Segmentación en materia de arquitectura, seguridad de la información y los lineamientos específicos de Servicios Ciudadanos Digitales:

> *“La entidad tiene definidos, implementados y probados periódicamente los planes de continuidad y disponibilidad de los servicios tecnológicos y las infraestructuras críticas que posee”,*

En virtud de lo anterior se hace prioritario la determinación de las actividades críticas que generarían perdida de la continuidad en la prestación de servicios institucionales y que son clave en la construcción del Plan de Continuidad de Negocio.

5. RECOMENDACIONES

A. Se requiere con prioridad la construcción, adopción y divulgación del Plan de Continuidad de Negocio debido a la ocurrencia de intermitencia en la prestación de servicios tecnológicos que impiden el desarrollo de las actividades institucionales tal como se ha evidenciado en los casos del 10 y 18 de agosto de 2020, éste último afectando la operación del sistema de Gestión Documental ORFEO, la intranet y la página web.

B. Es necesario recordar que el Plan de Continuidad del Negocio se encuentra entre los requerimientos establecidos en el Manual de Gobierno Digital, el cual hace parte del Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones el cual establece:

> *ARTÍCULO 2.2.9.1.2.2. Manual de Gobierno Digital. Para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de esta Política de Gobierno Digital, el cual será elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en coordinación con el Departamento Nacional de Planeación.*

C. Es necesario priorizar la actualización de los siguientes documentos institucionales que no se relacionan con las actuales medidas de trabajo en casa y riesgos asociados a la emergencia sanitaria COVID-19:

- Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información
- Plan de Seguridad y Privacidad de la Información
- Política de seguridad de la información

D. Realizar el análisis de las solicitudes que fueron atendidas fuera de tiempo basado en el Acuerdo de Nivel de Servicio ANS, con el fin de garantizar el cumplimiento del

tiempo establecido para la atención futuras de solicitudes, se sugiere realizar un análisis detallado que permita determinar acciones para evitar dichos incumplimientos.

E. Se hace necesario evidenciar la construcción del mapa de riesgos actualizado para el Área de Tecnología.

F. Se recomienda incluir dentro de los riesgos y controles (Numeral 4.6) de aquellas condiciones críticas que impidan la continuidad del negocio tal como los puede ser por ejemplo las fallas en el fluido eléctrico y determinar si es suficientemente mitigado a través del uso las plantas eléctricas de la sede principal, en razón a que se ha presentado intermitencia en la prestación de servicios de los sistemas de información debido a esta causa identificada, tal como fue informado por correo electrónico a la comunidad institucional el día 10 de agosto.

CARLOS ALBERTO QUITIÁN SALAZAR
Asesor de Control Interno
Instituto Distrital de las Artes

Elaboró: Giovanny Montenegro – Contratista Área de Control Interno