



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 1 de 35

1. INFORMACIÓN GENERAL

Proceso:	Gestión de Información y Tecnología
Dependencia:	Dirección de Gestión de Información y Tecnología
Tipo de auditoria o seguimiento:	Auditoria de Calidad y Ambiental
Fecha entrega del Informe	24 de julio de 2024

2. OBJETIVOS DE LA AUDITORIA O SEGUIMIENTO

Verificar que las actividades asociadas al proceso de Gestión de Información y Tecnología se desarrollen cumpliendo con los requerimientos de las normas ISO 9001:2015, ISO 14001:2015 y demás requisitos de la entidad. Igualmente, verificar la aplicación de los lineamientos transversales establecidos en los procesos de Gestión Documental y Evaluación y Mejora de la Gestión.

3. ALCANCE DE LA AUDITORIA O SEGUIMIENTO

La auditoría abarca los procesos de Gestión de Información y Tecnología aplicando las actividades relacionadas durante el periodo comprendido entre el 1 abril de 2023 y el 15 de junio de 2024. La auditoría se realizará del 21 al 28 de junio de 2024 de acuerdo con los requisitos aplicables al proceso de la norma ISO 9001:2015 & ISO 14001:2015, comprenderá el ciclo PHVA de la caracterización y documentos asociados a los procesos, y sus procedimientos. La auditoría se desarrollará teniendo en cuenta el procedimiento MC-PT-012 - Auditorías internas a los sistemas de gestión ejecutadas por la segunda línea de defensa. Los requisitos aplicables al proceso a auditar serán los definidos en el Manual del Sistema Integrado de Gestión AS-MA-001, versión vigente a la fecha y los que el equipo auditor considere pertinentes. En la auditoría se revisará la aplicación de los lineamientos de los procesos de Gestión Documental (manejo documental del archivo) y de Evaluación y Mejora de la Gestión

4. ACTIVIDADES DESARROLLADAS

Con el objeto de evaluar el cumplimiento de los requisitos 4.4.1 - 4.4.2- 5.2.2- 6.1-6.2- 7.1.3 -7.1.6 -7.5.3-1- 9.1.1- 9.1.3 -10 , de la NTC ISO 9001:2015 y los requisitos,5.2.2- 6.1.2-6.1.4- 6.2- 8.1-10 de la ISO 14001:2015 se realizó una entrevista y revisión documental con el objeto de conocer si el proceso se encuentra al tanto de la planeación estratégica de la Entidad, la política del Sistema Integrado de Gestión, la política del Sistema de Gestión Ambiental, caracterización del proceso, gestión del riesgo, indicadores de gestión e información documentada del que hacer de sus actividades claves, así como también las mejoras implementadas por el proceso para fortalecer su gestión.

El equipo auditor realizó jornadas de trabajo y tomo como documentos base de estudio para la auditoría los siguientes:

- Caracterización del proceso CÓDIGO: IT-PR-02 en su versión 10.
- Plan de compras
- Planes de mejoramiento
- Matriz de aspectos ambientales CÓDIGO: AS-FO-003
- Indicadores del proceso

Elaboró: Olga Milena Mendoza

FV: 20/05/2020



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 2 de 35

- Mapa de Riesgos Integrado CÓDIGO: DE-FO-032 en su versión 2.
- Manual de Seguridad y Privacidad de la Información IT-MA-002 V-8.
- Procedimiento IT-PT-023 Gestión de Información y Tecnología manejo de incidentes de seguridad y privacidad de la información con o sin afectación de datos personales.
- Procedimiento IT-PT- 017 Gestión de disponibilidad -v6
- Instructivo IT-IN-004 Gestión de Vulnerabilidad.
- Tabla de Retención Documental de la Dirección GD-FO-03 Versión 10 vigente.

4.1. CARACTERIZACIÓN DEL PROCESO.

El equipo auditor realiza un estudio y análisis minucioso de dicho documento, realiza una serie de preguntas, de su objetivo y alcance, así como preguntas relacionadas con el Planear, Hacer, Verificar y Actuar del proceso, con el fin de tener una claridad más amplia de conocimiento de la gestión realizada por el mismo.

Se evidencia que las entradas y salidas de la gestión del proceso de la Dirección de Gestión de Información y Tecnología tienen relación con la información documentada en la Caracterización de proceso, así como la relación que tienen con las demás áreas de la Entidad.

De igual forma para el equipo auditor es claro el conocimiento y apropiación que los auditados tienen acerca del conocimiento de su proceso.

4.2. PLAN DE COMPRAS

El equipo auditor analiza el plan de compras de los años 2023 y 2024, toma los tres más grandes del año 2023 así:

- En el plan anual de compras del año 2023, se solicitó recursos por valor de \$ 2.200.000.000 para el proyecto de Adquirir, instalar, configurar, e implementar los servicios y puesta en marcha, con soporte técnico y garantía por 3 años, de dos nodos de hiperconvergencia Nutanix para el MRE. y se procede a preguntar, cómo fue esta ejecución, con quienes se realizó, ver evidencias de su ejecución.
- En el plan anual de compras del año 2023, se solicitó recursos por valor de \$ 2.059.000.000 para el proyecto Adquisición solución de backup hiperconvergente, a lo que se pregunta cómo fue esta ejecución, con quienes se realizó, ver evidencias de su ejecución.
- En el plan anual de compras del año 2024, se solicitó recursos por valor de \$ 1.881.455.880, para el Servicio de soporte a usuarios de tecnologías de información a través de mesa de ayuda y mantenimiento preventivo y correctivo con suministro de repuestos, dejar ver carpeta del mismo contrato y sus informes trimestrales y su reporte en el SECOP II.

Se escucha como respuesta por parte de la funcionaria encargada del plan de compras que estos no fueron llevados a cabo, por razones de tiempo y de directrices de la administración de turno que impidieron su ejecución.

Para el año 2024 se indaga por el proyecto de inversión:

Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 3 de 35

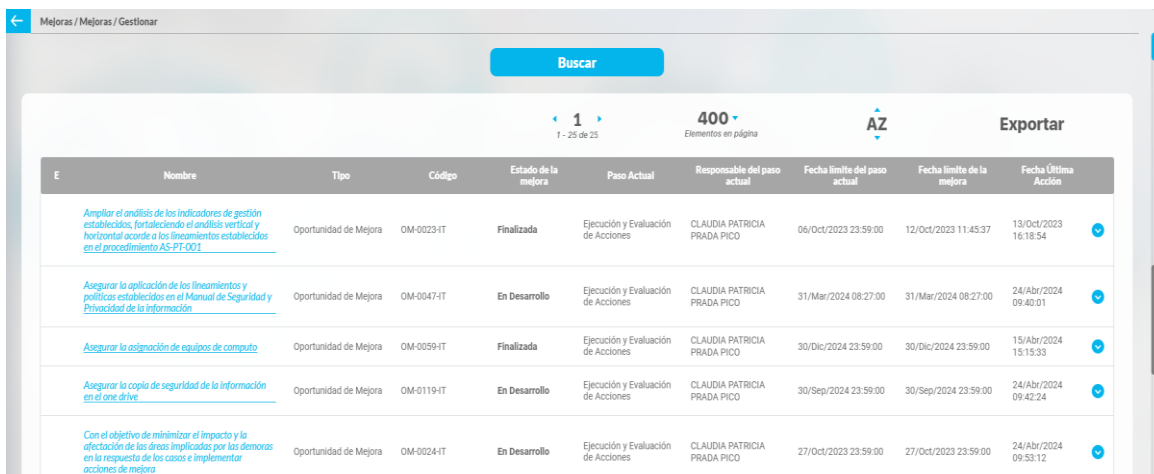
- Se tiene un proyecto de inversión con ficha BPIN 20230000000156 Transformación digital del Ministerio de Relaciones Exteriores por valor de \$ 20.000.000.000, cuyo objeto es: Renovar e incrementar la capacidad para garantizar la disponibilidad, continuidad, control de amenazas y efectividad de los servicios tecnológicos. Se indaga sobre el estado de su avance.

A lo que el equipo auditado realiza una explicación, clara y concisa en donde se muestra el proyecto de inversión y sus diferentes actividades que lo conforman de igual forma explica el estado de su ejecución, de forma satisfactoria para el equipo auditor.

4.3. PLANES DE MEJORAMIENTO

Se procede a indagar acerca de si el proceso durante el tiempo de esta auditoria suscribió planes de mejoramiento, a lo que los auditados informaron que si se suscribieron planes de mejoramiento producto de auditoría interna y tres más producto de incidentes de seguridad reportados.

Se procede a su revisión en el SUIT VISIÓN EMPRESARIAL, de manejo documental de la entidad, su análisis de causas y su plan de actividades para su manejo y posible solución.



E	Nombre	Tipo	Código	Estado de la mejora	Paso Actual	Responsable del paso actual	Fecha límite del paso actual	Fecha límite de la mejora	Fecha Última Acción
	Ampliar el análisis de los indicadores de gestión establecidos, fortaleciendo el análisis vertical y horizontal acorde a los lineamientos establecidos en el procedimiento AS-PT-001	Oportunidad de Mejora	OM-0023-HT	Finalizada	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	06/Oct/2023 23:59:00	12/Oct/2023 11:45:37	13/Oct/2023 16:18:54
	Asegurar la aplicación de los lineamientos y políticas establecidos en el Manual de Seguridad y Privacidad de la información	Oportunidad de Mejora	OM-0047-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	31/Mar/2024 08:27:00	31/Mar/2024 08:27:00	24/Abr/2024 09:40:01
	Asegurar la adquisición de equipos de computo	Oportunidad de Mejora	OM-0059-HT	Finalizada	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	30/Dic/2024 23:59:00	30/Dic/2024 23:59:00	15/Abr/2024 15:15:39
	Asegurar la copia de seguridad de la información en el one drive	Oportunidad de Mejora	OM-0119-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	30/Sep/2024 23:59:00	30/Sep/2024 23:59:00	24/Abr/2024 09:42:24
	Con el objetivo de minimizar el Impacto y la afectación de las áreas implicadas por los demoras en la respuesta de los casos e implementar acciones de mejora	Oportunidad de Mejora	OM-0024-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	27/Oct/2023 23:59:00	27/Oct/2023 23:59:00	24/Abr/2024 09:53:12

Elaboró: Olga Milena Mendoza

FV: 20/05/2020



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 4 de 35

Mejoras / Mejoras / Gestionar									
acciones de mejora									
Es importante que se fortalezca la socialización de la política de tratamiento de la información	Oportunidad de Mejora	OM-0053-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	31/Dic/2024 23:59:00	31/Dic/2024 23:59:00	15/Abr/2024 15:51:45	✓
Es importante que se fortalezca la socialización de la política de tratamiento de la información Embajada en Vietnam	Oportunidad de Mejora	OM-0069-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	26/Jun/2024 23:59:00	26/Jun/2024 23:59:00	15/Abr/2024 16:04:10	✓
Establecer la incorporación del formato AS-FO-007 como parte la verificación del destino final de los RAEE. Realizar una mesa de trabajo con todos los involucrados. Solicitar acompañamiento de la OAPDO.	Oportunidad de Mejora	OM-0027-HT	Finalizada	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	24/Nov/2023 23:59:00	24/Nov/2023 23:59:00	23/Ene/2024 19:07:21	✓
Fortalecer el uso adecuado de los formatos a través de los cuales se registran todas las actividades de la mesa de ayuda.	Oportunidad de Mejora	OM-0137-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	15/Ago/2024 23:59:00	15/Ago/2024 23:59:00	07/Jun/2024 09:36:15	✓
Fortalecer la implementación e interiorización del Manual de Seguridad y Privacidad de la Información	Oportunidad de Mejora	OM-0109-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	30/Jun/2024 23:59:00	30/Jun/2024 23:59:00	24/Abr/2024 10:00:03	✓
Incidente 145970 de protección de datos dado que se presentó la exposición de datos personales debido a que el enlace de consulta para el trámite de visas	No Conformidad	NC-0165-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	28/Mar/2025 23:59:00	28/Mar/2025 23:59:00	07/Jun/2024 09:40:24	✓

Mejoras / Mejoras / Gestionar									
Incidente de seguridad de la Información 145717 por pérdida de la grabación de una audiencia de un proceso disciplinario.	No Conformidad	NC-0168-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	28/Jun/2024 23:59:00	28/Jun/2024 23:59:00	07/Jun/2024 09:45:44	✓
Incidente vulneración de credenciales No. 145678 Hallazgo de incidente de la información donde fue comprometida / hackeada la cuenta de usuario de un funcionario.	No Conformidad	NC-0163-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	31/Mar/2025 23:59:00	31/Mar/2025 23:59:00	15/Abr/2024 16:24:12	✓
Incidentes 145830 Bitácora de San Carlos y 146420 Hackeo página web	No Conformidad	NC-0172-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	31/Mar/2025 23:59:00	31/Mar/2025 23:59:00	07/Jun/2024 09:49:02	✓
Incidentes 145831 y 146140 presentados por la pérdida de equipo de cómputo portátil el 09 de marzo de 2023 y del teléfono celular institucional el 23 de enero de 2024	No Conformidad	NC-0102-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	30/Abr/2025 23:59:00	30/Abr/2025 23:59:00	15/Abr/2024 16:35:00	✓
IT-MA-002 Seguridad y Privacidad de la Información, Numeral 8.6.3 Retiro o ajuste de los derechos de acceso Los derechos de acceso a los servicios de TI	No Conformidad	NC-0029-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	30/Ago/2024 23:59:00	30/Ago/2024 23:59:00	24/Abr/2024 11:20:48	✓
Realizar campañas de concientización a los funcionarios de la cancillería para socializar los cambios respecto a el mantenimiento preventivo y la importancia de solicitarlo de forma periódica.	Oportunidad de Mejora	OM-0026-HT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	06/Oct/2023 23:59:00	12/Oct/2023 12:09:01	24/Abr/2024 11:37:18	✓
Realizar Funcionalidad [script] para validar y verificar que se mantenga la integridad de la información, verificando el proceso o las operaciones cuando se cambian variables dentro	Acciones Preventivas	AP-0016-HT	Nueva	Proyección de Acciones	KAREN ROSANA MENESES ROMERO			29/Nov/2023 09:39:23	✓

Elaboró: Olga Milena Mendoza

FV: 20/05/2020



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 5 de 35

Incidente de seguridad de la Información 145717 por pérdida de la grabación de una audiencia de un proceso disciplinario.	No Conformidad	NC-0168-IT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	28/Jun/2024 23:59:00	28/Jun/2024 23:59:00	07/Jun/2024 09:45:44	✓
Incidente vulneración de credenciales No. 145678 Hallazgo de incidente de la información donde fue comprometida / hackeada la cuenta de usuario de un funcionario	No Conformidad	NC-0163-IT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	31/Mar/2025 23:59:00	31/Mar/2025 23:59:00	15/Abr/2024 16:24:12	✓
Incidentes 145830 Bitácora de San Carlos y 146420 Hackeo página web	No Conformidad	NC-0172-IT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	31/Mar/2025 23:59:00	31/Mar/2025 23:59:00	07/Jun/2024 09:49:02	✓
Incidentes 145831 y 146140 presentados por la pérdida de equipo de cómputo portátil el 09 de marzo de 2023 y del teléfono celular institucional el 23 de enero de 2024	No Conformidad	NC-0162-IT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	30/Abr/2025 23:59:00	30/Abr/2025 23:59:00	15/Abr/2024 16:35:00	✓
IT-MA-002 Seguridad y Privacidad de la Información, Numeral 8.6.3 Retiro o ajuste de los derechos de acceso Los derechos de acceso a los servicios de TI	No Conformidad	NC-0029-IT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	30/Ago/2024 23:59:00	30/Ago/2024 23:59:00	24/Abr/2024 11:20:48	✓
Realizar campañas de concientización a los funcionarios de la cancillería para socializar los cambios respecto a el mantenimiento preventivo y la importancia de solicitarlo de forma periódica	Oportunidad de Mejora	OM-0026-IT	En Desarrollo	Ejecución y Evaluación de Acciones	CLAUDIA PATRICIA PRADA PICO	06/Oct/2023 23:59:00	12/Oct/2023 12:09:01	24/Abr/2024 11:37:18	✓
Realizar Funcionalidad (script) para validar y verificar que se mantenga la integridad de la información, verificando el proceso o las operaciones cuando se cambian variables dentro	Acciones Preventivas	AP-0016-IT	Nueva	Proyección de Acciones	KAREN ROXANA MENESES ROMERO			29/Nov/2023 09:39:23	✓

Estos se están reportando por parte de su proceso para su seguimiento por parte de la oficina encargada para este fin.

4.4. MATRIZ DE ASPECTOS AMBIENTALES CODIGO AS-FO-003

Se procede a indagar acerca del conocimiento de la política ambiental, y de sus programas, por lo que los auditados proceden a hacer una breve descripción e interpretación de la política de forma clara para los auditores, de igual forma realizan una descripción de los programas ambientales, y se solicita información acerca del aporte que realiza el proceso al sistema.

El equipo auditor realiza inspección visual al punto ecológico ubicado en la dirección y se ve que esta al momento de su auditoria bien utilizado, por lo que se hace importante seguir haciendo seguimiento a su correcta utilización.

De igual forma se procede a revisar todas las canecas de uso personal en cada puesto de trabajo, a lo que el equipo auditor encontró mal uso de estas en tres de ellas, ya que se encontraba papel de trabajo roto y revuelto con bolsas de papel y palillos de cafetería, en otras dos se encontró botellas plásticas.

En alcance a la auditoría interna con relación al Sistema de Gestión Ambiental, se solicita adjuntar la evidencia correspondiente a la última certificación de RAEES entregados para gestión a la empresa que actualmente tiene convenio con el Ministerio.

Se adjunta:

Certificado para la gestión, tratamiento y aprovechamiento de residuos de aparatos eléctricos, electrónicos, no aprovechables y peligrosos por parte de PCSHEK TECNOLOGÍA Y SERVICIOS SAS.

Resolución DGEN No. 20217000183 de 23 ABR. 2021,"Por la cual se otorga una licencia ambiental y se toman otras

Elaboró: Olga Milena Mendoza

FV: 20/05/2020



TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 6 de 35

determinaciones". Resolución que otorga la CAR a la empresa para la gestión de RAEES.

 PCSHEK Reacondicionamos por Naturaleza	CERTIFICADO PARA LA GESTIÓN, TRATAMIENTO Y APROVECHAMIENTO DE RESIDUOS DE APARATOS ELÉCTRICOS, ELECTRÓNICOS, NO APROVECHABLES Y PELIGROSOS.	Código: COL-ADM-F-06
		Versión: 7
		Vigencia: 01/02/2023
		Páginas: 1 de 1

PCSHEK TECNOLOGIA Y SERVICIOS SAS
NIT. 900.413.420-8

Certificado N° CG8194 RLGA- CO-TB-
08142023- RAEECANCILLERÍA BTA

Certifica que realizó el proceso de **recolección, transporte y gestión integral** de todos los elementos relacionados a continuación, en pleno cumplimiento de la normatividad ambiental vigente:

GENERADOR: MINISTERIO DE RELACIONES EXTERIORES
 EMAIL: Deivis.Talero@cancilleria.gov.co
 NIT: 899999042-9
 DIRECCIÓN: Calle 10 No 5 – 51 BOGOTÁ BOGOTÁ
 No. ENTRADA: 14091

FECHA DE CERTIFICACIÓN: 18/09/2023

TRATAMIENTO DE RESIDUOS							
FECHA DE RECOLECCION	FECHA DE GESTION	RESIDUO	Clasificación	CANT (KILOS)	CANT (UNID)	PROCESO / TRATAMIENTO	GESTOR AMBIENTAL
2023-09-11	2023-09-18	ELECTRÓNICA Y EQUIPOS DE TELECOMUNICACIONES/PERIFÉRICOS, PARTES Y TARJETAS PARA COMPUTADORES E/ TECLADO	A1180	8.0	12	ALMACENAMIENTO / APROVECHAMIENTO	PCSHEK
9/6/2023	9/13/2023	ELECTRÓNICA Y EQUIPOS DE TELECOMUNICACIONES/PERIFÉRICOS, PARTES Y TARJETAS PARA COMPUTADORES E/DISCO SATA	A1180	13.0	33	ALMACENAMIENTO / APROVECHAMIENTO	PCSHEK
9/6/2023	9/13/2023	ELECTRÓNICA Y EQUIPOS DE TELECOMUNICACIONES/ COMPUTADORES Y EQUIPOS PARA TRATAMIENTO DE DATOS/ CELULAR	A1180	1.0	2	ALMACENAMIENTO / APROVECHAMIENTO	PCSHEK
9/6/2023	9/13/2023	ELECTRÓNICA Y EQUIPOS DE TELECOMUNICACIONES /PERIFÉRICOS, PARTES Y TARJETAS PARA COMPUTADORES E/ CABLE VARIADO	A1180	12.0	2	ALMACENAMIENTO / APROVECHAMIENTO	PCSHEK
9/6/2023	9/13/2023	MAQUINARIA Y EQUIPO ELÉCTRICO PILAS Y ACUMULADORES (PILAS SECUNDARIAS O BATERÍAS RECARGABLES) /BATERÍAS DE LITIO (ion litio, Li-Ion)	Y23	3.0	3	ALMACENAMIENTO / APROVECHAMIENTO	GSOLUTIONS

Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 7 de 35

4.5. INDICADORES DE GESTIÓN

Se indaga acerca de los indicadores reportados en el SUIT EMPRESARIAL, a lo que el auditado procede a mostrar sus resultados de la última medición realizada en el año 2024 así como el análisis de estos, el equipo auditor indaga sobre las variables que conforman los respectivos indicadores y la procedencia de estos.

Nombre Indicador	Variabes Indicador - Fórmula	Frecuencia	Meta vs. resultado
Nivel de cumplimiento en el desarrollo de los Sistemas de Información (IG)	(Número de requerimientos de desarrollo de software atendidos/Número total de requerimientos de desarrollo de software planeados en el periodo) *100	Cuatrimestral	85% - 83.33% - Aceptable
Uso y apropiación de herramientas de productividad de TI (IG)	(Promedio de usuarios que usan las herramientas de productividad de TI disponibles/Cantidad de usuarios habilitados en las herramientas de productividad de TI) *100	Trimestral	80% - 94.81% - Satisfactorio
Cumplimiento de los niveles de atención de incidentes de servicios TI (IG)	(Número de incidentes de TI atendidos dentro de ANS/Total de incidentes de TI atendidos) *100	Trimestral	90% - 93.05% - Satisfactorio
Satisfacción usuarios mesa de ayuda (IG)	(Cantidad de usuarios satisfechos/Cantidad total de usuarios encuestados) *100	Trimestral	92% - 97.49% - Satisfactorio
Nivel de disponibilidad de los servicios tecnológicos (IG)	((Total de Horas acordadas del servicio-Horas presentadas de interrupción) /Total de Horas acordadas del servicio) *100	Cuatrimestral	99% - 99.78% - Satisfactorio

Todos los indicadores cumplen con su respectivo análisis, de igual forma se revisa el análisis de tendencia reportado en el mes de enero de 2024.



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 8 de 35

4.6. MAPA DE RIESGOS

Riesgo	Clasificación
Posibilidad de afectación económica por la indisponibilidad de los servicios de tecnología de la información y comunicaciones asociados a trámites y servicios	Seguridad y Privacidad de la Información
Posibilidad de afectación reputacional por la pérdida de integridad de la información de la Entidad.	Seguridad y Privacidad de la Información
Posibilidad de afectación reputacional por la pérdida de confidencialidad de la información reservada y confidencia	Seguridad y Privacidad de la Información
Posibilidad de afectación reputacional por adulterar o hacer mal uso de la información institucional, en beneficio propio o de terceros.	Corrupción

El equipo auditor indaga sobre los riesgos identificados por el proceso y su reporte de avance del primer cuatrimestre del año 2024, se evidencia su cumplimiento y se solicitan evidencias de las acciones de control.

4.7. DOCUMENTOS DEL PROCESO

- Manual de Seguridad y Privacidad de la Información IT-MA-002 V-8.
- Procedimiento IT-PT-023 Gestión de Información y Tecnología manejo de incidentes de seguridad y privacidad de la información con o sin afectación de datos personales.
- Procedimiento IT-PT- 017 Gestión de disponibilidad -v6
- Instructivo IT-IN-004 Gestión de Vulnerabilidad.

El equipo auditor para cada uno de estos documentos realiza estudio completo de los mismos e indaga acerca del objetivo y alcance de estos, así como sus políticas de operación y puntos de control, para la mayoría de estas consultas se solicita evidencia de la misma la cual es mostrada y entregada de forma satisfactoria para el equipo auditor.

4.8 Revisión de Procedimientos

4.8.1. Procedimiento IT-IN-004 Gestión de Vulnerabilidad

El Oficial de Seguridad y Privacidad de la Información es el responsable de explicar las actividades descritas en el instructivo IT-IN-004, en el desarrollo de ejercicio se realizó la descripción de los objetivos y alcance de este instructivo.

Se inicio explicando las diferentes fases para el análisis, remediación y mitigación de vulnerabilidades. Con respecto a la fase de planeación se consolida la información en un archivo Excel con el fin de realizar un escaneo y seguimiento correspondiente de acuerdo con el análisis de vulnerabilidad el cual se realiza en 1. Forma Mensual a través de dos herramientas una de las cuales es Especializada en equipo de infraestructura la cual se realizó hasta diciembre del 2023, este año no se realiza debido a que no hay contrato. Y la segunda herramienta es especializada en análisis de códigos. El análisis de vulnerabilidad lleva un registro con el reporte de vulnerabilidad. Anexa Informe mensual archivo Excel de diciembre 2023 y marzo de 2024

Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 9 de 35

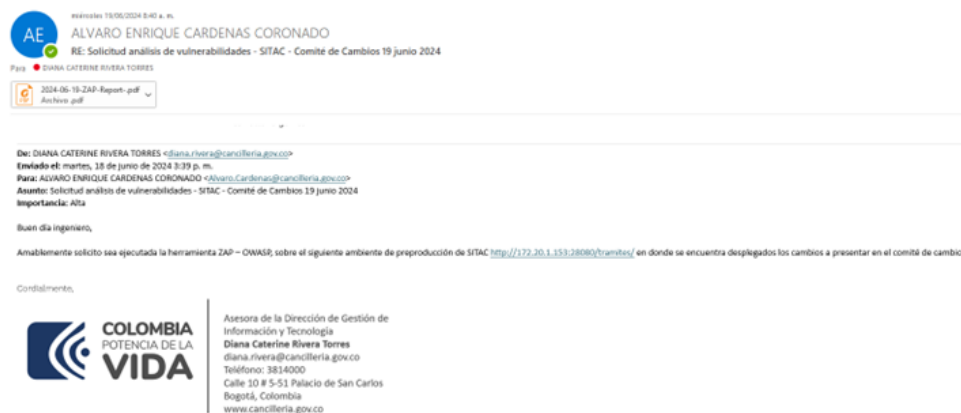
Diciembre 2023.

Nombre	Responsable	Criticas	Altas	Medias	Bajas	Criticas A	Altas A	Medias A	Bajas A	Criticas N	Altas N	Medias N	Bajas N	Mes	Mes Escrito
Servidores Telefonía	GIT de Servicios Tecnológicos	2	2	16	11	2	2	16	11	0	0	0	0	0	31/12/2022 diciembre
Servidores Windows 2003	GIT de Servicios Tecnológicos	9	19	25	3	9	19	25	2	0	0	0	0	1	31/12/2022 diciembre
Servidores Windows 2008	GIT de Servicios Tecnológicos	280	996	688	87	261	982	631	69	19	14	57	18	18	31/12/2022 diciembre
Servidores Windows 2012	GIT de Servicios Tecnológicos	328	1016	1591	261	272	972	1562	214	56	44	29	47	47	31/12/2022 diciembre
Servidores Windows 2016	GIT de Servicios Tecnológicos	193	567	662	97	175	548	658	78	18	19	4	19	19	31/12/2022 diciembre
Servidores Windows 2019	GIT de Servicios Tecnológicos	115	93	247	43	88	59	231	29	27	34	16	14	14	31/12/2022 diciembre
Servidores Windows otros	GIT de Servicios Tecnológicos	5	1	49	3	5	1	49	3	0	0	0	0	0	31/12/2022 diciembre
Servidores Linux	GIT de Servicios Tecnológicos	194	451	749	128	194	451	747	128	0	0	2	0	0	31/12/2022 diciembre
Equipos de comunicación	GIT de Servicios Tecnológicos	7	3	43	81	7	3	43	81	0	0	0	0	0	31/12/2022 diciembre
Fax e impresora	GIT de Servicios Administrativos- Cesar Cufiño	18	54	16	1	17	53	16	1	1	1	0	0	0	31/12/2022 diciembre

Marzo 2024

Sistema
Protocolo- https://protocolo.cancilleria.gov.co/Protocolo/
Caribu - https://servicioexterior.cancilleria.gov.co/caribu/
Ausentismo - https://servicioexterior.cancilleria.gov.co/ausentismo/
Sigueme - https://servicioexterior.cancilleria.gov.co/sigueme/
SISE - https://servicioexterior.cancilleria.gov.co/sise/
Certificaciones - https://sinmre.cancilleria.gov.co/Certificaciones/inicio.aspx
SINMRE-login - https://sinmre.cancilleria.gov.co/login.aspx
Simple - https://servicioexterior.cancilleria.gov.co/simple/
Acceso Servicios TI - https://tramites.cancilleria.gov.co/AccesoServiciosTI/Cuenta/IniciarSesion?ReturnUrl=http://c3.cancilleria.gov.co:8080/c3slvisor.aspx
Directorios Funcionarios - https://directorios.cancilleria.gov.co/Directorios/Funcionarios.aspx
http://c3.cancilleria.gov.co:8080/c3slvisor.aspx
c3ppal.cancilleria.gov.co:8082/c3sl.aspx

2. Gestión de cambios son análisis de vulnerabilidad en el cumplimiento de habilitación de cambios IT-PT-022 se realizan el requerimiento mediante correo electrónico por el responsable de cambio. Anexa correos en que los ingenieros solicitan el reporte de vulnerabilidades para la gestión de cambios.



AE Mensaje 19/06/2024 8:40 a. m.
ALVARO ENRIQUE CARDENAS CORONADO
 RE: Solicitud análisis de vulnerabilidades - SITAC - Comité de Cambios 19 junio 2024
 Para: DIANA CATERINE RIVERA TORRES
 2024-06-19-ZAP-Report.pdf
 Archivo.pdf

De: DIANA CATERINE RIVERA TORRES <diana.rivera@cancilleria.gov.co>
 Enviado el: martes, 18 de junio de 2024 3:29 p. m.
 Para: ALVARO ENRIQUE CARDENAS CORONADO <Alvaro.Cardenas@cancilleria.gov.co>
 Asunto: Solicitud análisis de vulnerabilidades - SITAC - Comité de Cambios 19 junio 2024
 Importancia: Alta

Buen día ingeniero,

Amablemente solicito sea ejecutada la herramienta ZAP - OWASP, sobre el siguiente ambiente de preproducción de SITAC <http://172.20.1.153:28080/tramites/> en donde se encuentra desplegados los cambios a presentar en el comité de cambios.

Confidencialmente,


COLOMBIA POTENCIA DE LA VIDA
 Asesora de la Dirección de Gestión de Información y Tecnología
 Diana Catherine Rivera Torres
 diana.rivera@cancilleria.gov.co
 Teléfono: 3814000
 Calle 10 # 5-51 Palacio de San Carlos
 Bogotá, Colombia
 www.cancilleria.gov.co

En la fase 2. Se analiza las vulnerabilidades y se envía a los diferentes coordinadores responsables por correo electrónico.

Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 10 de 35

ANÁLISIS DE VULNERABILIDADES URLS EN PRODUCCION													
Julieth	Sistema	MARZO			ABRIL			MAYO			JUNIO		
		Alto	Medio	Bajo	Alto	Medio	Bajo	Alto	Medio	Bajo	Alto	Medio	Bajo
	Protocolo - https://protocolo.cancilleria.gov.co/Protocolo/	2	2	7	0	1	7	0	3	8	0	3	8
	Caribu - https://servicioexterior.cancilleria.gov.co/caribu/	1	3	8	1	2	8	1	3	8	0	3	8
	Ausentismo - https://servicioexterior.cancilleria.gov.co/ausentismo/	1	3	8	0	2	7	1	3	8	0	4	8
	Sigueme - https://servicioexterior.cancilleria.gov.co/sigueme/	1	5	9	1	7	10	1	7	10	1	6	9
	SISE - https://servicioexterior.cancilleria.gov.co/sise/	1	2	6	1	5	8	0	5	8	0	4	7
	Certificaciones - https://sinmre.cancilleria.gov.co/Certificaciones/inicio.aspx	0	3	7	1	4	9	1	3	7	0	3	7
	SINMRE-login - https://sinmre.cancilleria.gov.co/login.aspx	0	3	5	0	3	6	0	3	5	0	3	5
	Simple - https://servicioexterior.cancilleria.gov.co/simple/	1	3	6	2	5	9	1	6	8	0	5	7
	Acceso Servicios TI - https://tramites.cancilleria.gov.co/AccessoServiciosTI/Cuenta/IniciarSesion?ReturnU	0	2	9	1	3	10	0	3	10	0	2	9
	Directorios Funcionarios - https://directorios.cancilleria.gov.co/Directorios/Funcionarios.aspx	1	2	7	0	2	7	0	3	10	0	2	7
	c3 - http://c3.cancilleria.gov.co/8080/c3s/visor.aspx	0	3	2	0	3	2	0	3	2	0	3	2
	c3ppal - http://c3ppal.cancilleria.gov.co/8082/c3s1.aspx	0	3	3	0	3	3	0	3	3	0	3	3

Se explica la 3 fase corresponde a la Remediación o mitigación la cual se realiza de acuerdo con los criterios de tiempo según el correo reportado por el Especialista, si no es posible cumplir con los tiempos el responsable de la mitigación informará por correo antes del vencimiento del tiempo de remediación. Y si es posible mitigarla debe adjuntar plan de acción. **Anexo evidencia de Remediación.**

RV: DESK-15116 Reportes de vulnerabilidad OWASP-ZAP Mayo 2024



Buen día, Álvaro Cárdenas.

Me permito copiar el análisis y verificación realizada por parte del Proveedor Penesmos S.A sobre las vulnerabilidades reportadas.



De: Soporte SVE (SIVA) <soporte@penesmos.com>
Enviado el: miércoles, 12 de junio de 2024 11:32 a. m.
Para: MARIA VICTORIA MERA JARAMILLO <mera.mera@cancilleria.gov.co>
Asunto: DESK-15116 Reportes de vulnerabilidad OWASP-ZAP Mayo 2024

Luis Vargas comentó:

Revisamos el informe y notamos que no hay alertas de clasificación alta, solo medias y todas referidas a la directiva CSP que se implementó hace un tiempo y que ya han sido referidas en el pasado.

Al respecto le indicamos que de momento no podemos endurecer esta directiva más pues afectamos el funcionamiento de la SVE de cara a los usuarios.

Nuestra sugerencia es aceptar el riesgo asociado dado que en las pruebas que hemos realizado nosotros y ustedes en el pasado, al activar la protección XSS y el CSP no es posible explotar este hallazgo hasta ahora.

Después pasamos a la 4 fase de verificación por demanda o Retest donde después de realizado la remediación o mitigación se solicita por correo que se valide si la acción fue exitosa o debe realiza acciones adicionales. **Anexa evidencia de verificación.**



TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 11 de 35

Por último, está la 5 fase de los informes que elabora y presenta el especialista en el formato IT-FO-001 Informe de Evaluación Gestión Procesos de TI. **Anexo de evidencias de informes**

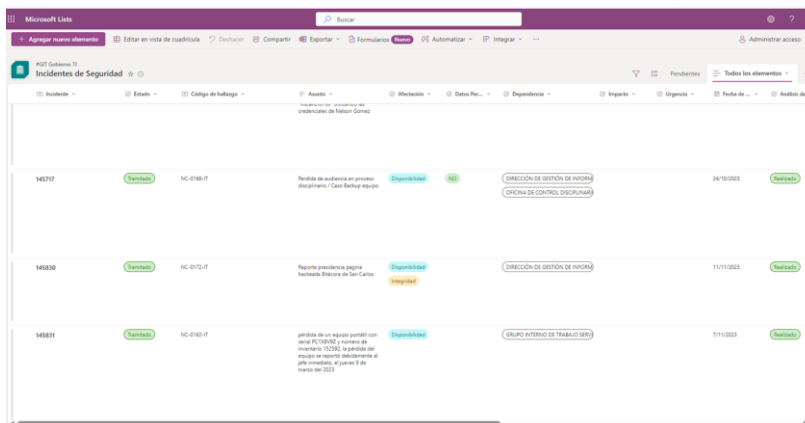


4.8.2. Procedimiento IT-PT-023 Gestión de Información y Tecnología Manejo de incidentes de seguridad y privacidad de la información con o sin afectación de datos personales.

El Oficial de Seguridad y Privacidad de la Información es el responsable explica los objetivos y alcance de este procedimiento.

Se pregunta sobre las políticas de operación lo correspondiente al equipo de atención a incidentes de seguridad de la información si existe un acto administrativo que establezca la conformación de este equipo donde se aclara que no tiene acto administrativo, este equipo se reúne cada vez que se presenta un incidente y definen el procedimiento de atención de acuerdo con la clase de incidente que se presenta, donde se deja documentado el manejo del incidente.

Ahora bien, se informa que los incidentes se centralizan a través de la herramienta de mesa de ayuda donde clasifica y escala al oficial de seguridad y privacidad de la información.



Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 12 de 35

Luego el Equipo Respuesta a incidentes realiza el estudio, análisis y lo clasifica de acuerdo con las categorías que tienen establecidas en el procedimiento (Acceso no autorizado, modificaciones de recursos no autorizados, indisponibilidad de acceso a información, incumplimiento al Manual de Políticas de Seguridad y Privacidad de la Información).

En cuanto a la política de operación 8.4 Evaluación establece que el Equipo de Respuesta a incidente establece el impacto, la urgencia que el incidente puede generar a la entidad, el procedimiento tiene definidos unos niveles de impacto y urgencia como son:

IMPACTO	NIVEL	TIPO DE INCIDENTE
CRITICO	4	El incidente afecta de manera total la continuidad de los procesos críticos de la entidad.
ALTO	3	El incidente afecta la continuidad de más de un proceso crítico de la entidad.
MEDIO	2	El incidente afecta la continuidad de un proceso crítico de la entidad.
BAJO	1	El incidente afecta la continuidad de un proceso NO crítico de la entidad.

Urgencia	Descripción
Urgente	El incidente requiere atención y recuperación de los procesos críticos afectados de forma inmediata.
Alta	El incidente requiere especial atención ya que ha afectado en forma parcial dos o más procesos críticos.
Normal	El incidente requiere atención media debido a que afecta la continuidad de un proceso crítico en forma parcial
Baja	El incidente no requiere atención urgente, no afecta la continuidad de ningún proceso crítico en la entidad.


Adicionalmente el Equipo Respuesta a incidentes debe indicar la prioridad en la atención del incidente

PRIORIDAD		URGENCIA			
		Baja	Normal	Alta	Urgente
IMPACTO		1	2	3	4
Critico	4	4	8	12	16
Alto	3	3	6	9	12
Medio	2	2	4	6	8
Bajo	1	1	2	3	4

En el acta de reunión CO-FO-05 que deja constancia la descripción del incidente las causas de ella y las estrategias a seguir no se evidencia que se relacione los niveles de impacto y urgencia que está establecida en el procedimiento para que después se establezca la prioridad en la atención del incidente.



TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 13 de 35

 **Ministerio de Relaciones Exteriores**
República de Colombia

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	ACTA REUNIÓN / LISTADO DE ASISTENCIA	VERSIÓN: 5
RESPONSABILIDAD POR APLICACIÓN:	TOCOS LOS PROCESOS, EMBAJADAS, CONSULADOS Y MINISTERIOS PERMANENTES DE COLOMBIA EN EL EXTERIOR	Página 1 de 3

1. DATOS GENERALES DE LA REUNIÓN

Asunto o Tema	Asesoría metodológica análisis de causas incidente 146420 Hackeo página Cancillería				
Acta de Reunión	X	Listado de Asistencia	X		
Fecha	10/05/2024	Hora Inicio	9:30	Hora Final	10:10
Presencial	No aplica	Virtual		Microsoft Teams	
Responsable:	Andrea del Pilar Rozo Castro				

2. DESARROLLO DE LA REUNIÓN

A través de la presente mesa de trabajo se lleva a cabo el acompañamiento metodológico orientado a la elaboración del análisis de causas en atención al hallazgo:

Incidente 146420 Hackeo página Cancillería
Incidente reportado el 09 de abril de 2024 por ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) el cual identifica el ataque de un hacker a las páginas "Patrimonio Arqueológico" y "Galio 40 aniversario" entre el 30 y 31 de enero de 2024.

Una vez aplicada la metodología de los 5 por qué se establecen que las causas que dieron lugar al incidente corresponden a dos de las causas raíz identificadas en el incidente "145830 BITACORA SAN CARLOS":

¿POR QUÉ?	¿POR QUÉ?	¿POR QUÉ?	¿POR QUÉ?	¿POR QUÉ?
El servicio salió a producción sin pruebas Microsoft Defender instalado	Incumplimiento del lineamiento 8.9.5 Protección contra código malicioso establecido en el Manual de Seguridad de la Información (IT-MA-002)	No existe una línea base de seguridad para los servidores en el procedimiento operativo correspondiente	No aplica	No aplica
La IP de los sitios publicados no aparece en	Incumplimiento IT-IN-004 Gestión de Vulnerabilidades con la weblogs relacionados con	No se encuentra un lineamiento operativo respecto al inventario de IP que administra la Oficial de Seguridad de la Información en sus		

4.8.3. Procedimiento IT-PT- 017 GESTIÓN DE DISPONIBILIDAD -V6

El funcionario encargado de este procedimiento procede a realizar una descripción acerca de su objetivo y alcance, de su objetivo afirma que se busca asegurar que los servicios de TI funcionen ininterrumpidamente y de manera fiable siempre que los usuarios deseen hacer uso de ellos, en el marco de los acuerdos de niveles de servicio vigentes.

De igual forma realiza una descripción de su alcance en donde aclara que inicia con cuantificar los requisitos de disponibilidad reales y termina con elaborar informe de gestión del proceso y proponer acciones de mejora.

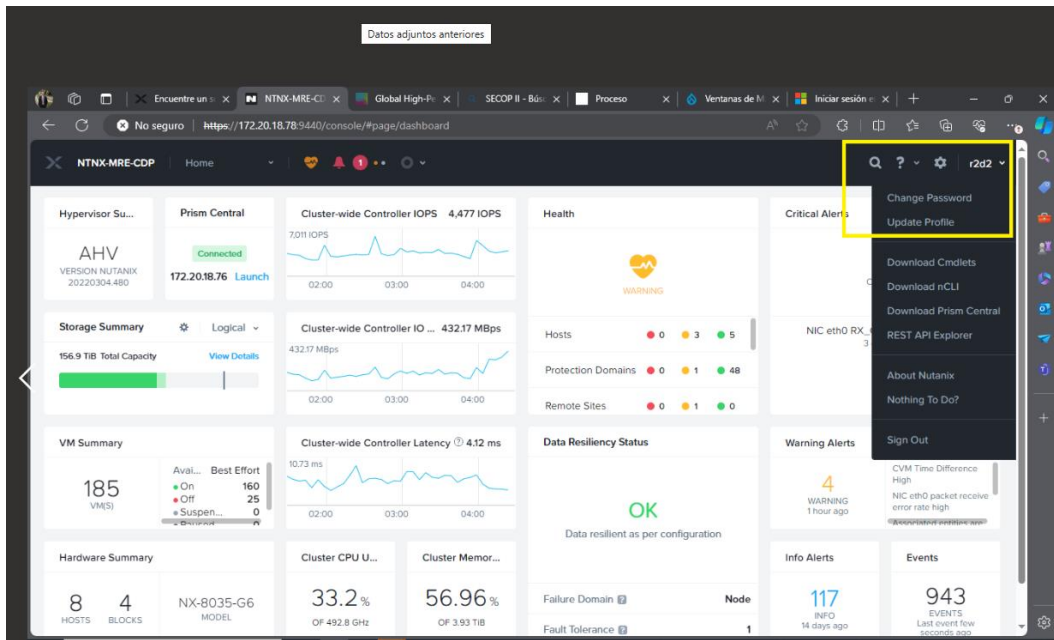
Hace una descripción del plan de trabajo que se realiza con el equipo de ingenieros para establecer el comportamiento de los diferentes sistemas de información, el cual se realiza a través de varias herramientas para tal fin, estas son mostradas de manera virtual y se da explicación por parte del auditado del funcionamiento de estas.

Herramienta NTN-X-MRE-CDP

Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 14 de 35



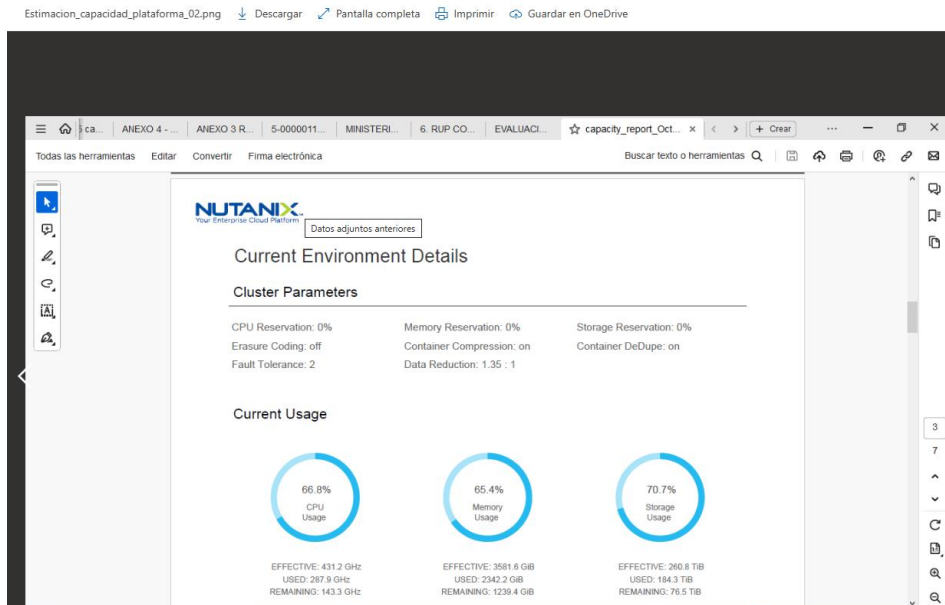
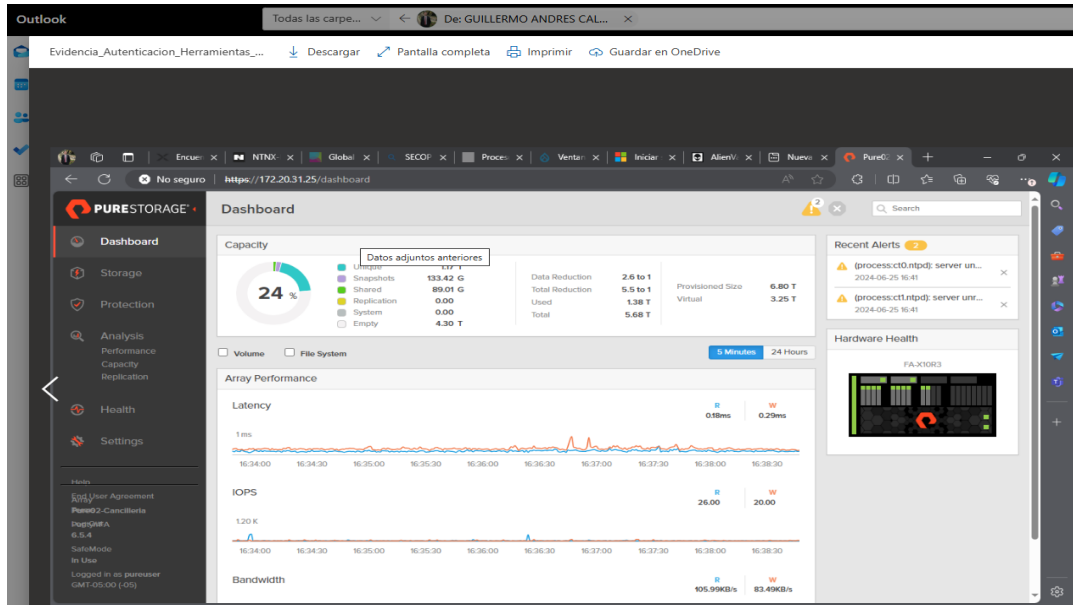
Esta herramienta visualiza el comportamiento en tiempo real de cada uno de los aplicativos de la entidad.



Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 15 de 35



Elaboró: Olga Milena Mendoza

FV: 20/05/2020



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 16 de 35

Se solicitan evidencias relacionadas con el proceso de Gestión de Disponibilidad y el procedimiento del cálculo del indicador, las cuales se observan en tiempo real.

Análisis Indisponibilidad Cuatrimestre_Enero-Abril2024.xlsx

- Indisponibilidad_Servicios_TI_Enero-Abril2024.xlsx
- Indicador de disponibilidad Cuatrimestre Enero - Abril 2024.msg
- Trazabilidad_Calculo_Tiempos_incidentes_Disponibilidad_Aranda_01.png
- Trazabilidad_Calculo_Tiempos_incidentes_Disponibilidad_Aranda_02.png
- Trazabilidad_Calculo_Tiempos_incidentes_Disponibilidad_Aranda_03.png

Evidencias relacionadas con la programación de las ventanas de mantenimiento del año 2024:

- Evidencia_Programacion_Ventanas_Mantenimiento_2024_correo.png
- Evidencia_Programacion_Ventanas_Mantenimiento_2024_Intranet.png

Evidencia de la autenticación de ingreso para todas herramientas de Monitoreo utilizadas por el grupo de Servicios Tecnológicos:

- Evidencia_Autenticacion_Herramientas_Monitoreo.png
- Evidencia_Autenticacion_Herramientas_Monitoreo_02.png
- Evidencia_Autenticacion_Herramientas_Monitoreo_03.png
- Evidencia_Autenticacion_Herramientas_Monitoreo_04.png
- Evidencia_Autenticacion_Herramientas_Monitoreo_05.png
- Evidencia_Autenticacion_Herramientas_Monitoreo_06.png
- Evidencia_Autenticacion_Herramientas_Monitoreo_07.png
- Evidencia_Autenticacion_Herramientas_Monitoreo_08.png
- Evidencia_Autenticacion_Herramientas_Monitoreo_09.png

Evidencia de la utilización de las herramientas para cálculo de la capacidad y la viabilidad para garantizar la disponibilidad de los sistemas de información:

- Estimacion_capacidad_plataforma_01.png
- Estimacion_capacidad_plataforma_02.png
- Estimacion_capacidad_plataforma_03.png
- Estimacion_capacidad_plataforma_04.png

De igual forma estos datos son descargados y analizados en matrices de Excel.

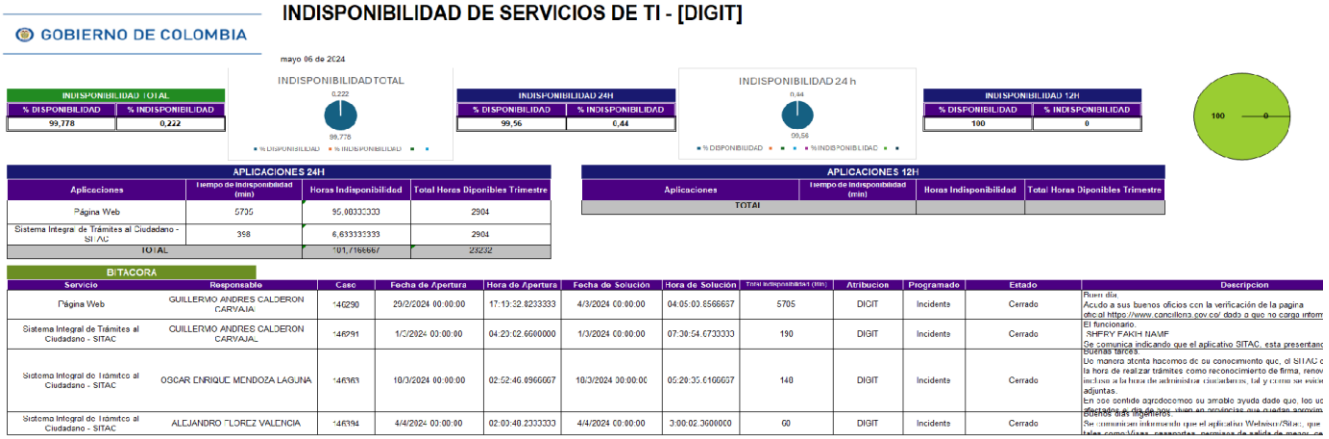
Elaboró: Olga Milena Mendoza

FV: 20/05/2020



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 17 de 35



ANÁLISIS INDISPONIBILIDAD INDICADORES DE GESTIÓN SERVICIOS TECNOLÓGICOS CUATRIMESTRE Enero -Abril 2024

INDICADOR	% DISPONIBILIDAD	% INDISPONIBILIDAD	ANÁLISIS	CAUSAS DE INDISPONIBILIDAD	ACCION DE MEJORA
Aplicaciones 7x24	99,56	0,44	De las aplicaciones y servicios a las cuales se les monitorea sus niveles de disponibilidad y que tienen disponibilidad las 24 H, se presentaron eventos de indisponibilidad para el sistema SITAC y para la pagina web. De un total de 23.232 horas de disponibilidad esperada, se presentaron 101,72 horas de indisponibilidad.	Las indisponibilidades fueron ocasionadas por inconvenientes en el sistema SITAC y en el servicio de Pagina Web. La intermitencia en el servicio de la pagina www.cancilleria.gov.co se genero por el cambio del proveedor del servicio DNS, cambio que fue necesario ejecutar por el vencimiento del contrato con el proveedor cloudflare, se configuro un servicio de DNS en Microsoft Azure. Este cambio en los nuevos servidores de DNS se demoro en replicar en todos los proveedores de servicios de internet a nivel mundial, por ellos en algunos lugares del mundo la pagina funcionaba, en otros la pagina no cargaba. Para el caso del SITAC, las interrupciones, fueron ocasionadas en dos ocasiones por una falla en el componente del bus de servicios, en otra ocasion se implemento en produccion un par de nodos de aplicacion con una versión con sistema operativo SUSE 11 SP3, con el fin de verificar la funcionalidad de esos dos servidores en produccion, sin embargo en la madrugada del 01/03, se recibieron reportes de los usuarios que eran dirigidos por el F5 hacia esos nodos, presentando problemas de autenticación y tampoco los cargaba ciertas opciones de menú.	Para el caso del Inconveniente de la pagina web, fue necesario esperar a que el cambio en los DNS replicara a nivel mundial. Para las fallas de SITAC en dos casos, se aplico el protocolo de reinicio de todo el Bus de Servicios, para poder restablecer el servicio. En el tercer caso fue necesario remover esos dos servidores del pool del balanceo en el F5 y restaurar los servidores afectados con una versión de OS SUSE 12 SP4

Elaboró: Olga Milena Mendoza

FV: 20/05/2020



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 18 de 35

Aplicaciones 5x8	100,00	0,00	Las aplicaciones/servicios a las cuales se les monitorea sus niveles de disponibilidad y que tienen disponibilidad las 12 H, no presentaron eventos de indisponibilidad para el periodo. Dentro de un total de 22.632 horas de disponibilidad esperada, hubo 0 horas de indisponibilidad	NA	NA
Aplicaciones 24 H			Aplicaciones 7x24		
Aplicaciones	Periodo Indisponibilidad	Horas Indisponibilidad	Total Horas Disponibles Trimestre	Horas Disp. x mes	Mes
SITAC	338 min	5,63	2904	744	Enero
APOSTILLA	0,0	0,00	2904	696	Febrero
INTERNET	0,0	0,00	2904	744	Marzo
PAGINA WEB	5705 min	95,08	2904	720	Abril
DIGITURNO Y AGENDAMIENTO	0,0	0,00	2904		
MESA DE AYUDA	0,0	0,00	2904		
CALL CENTER	0,0	0,00	2904		
TELEFONIA IP	0,0	0,00	2904		
		101,72	23232	2904	Total

Los festivos no importan, solo si el mes tiene 30 o 31 días

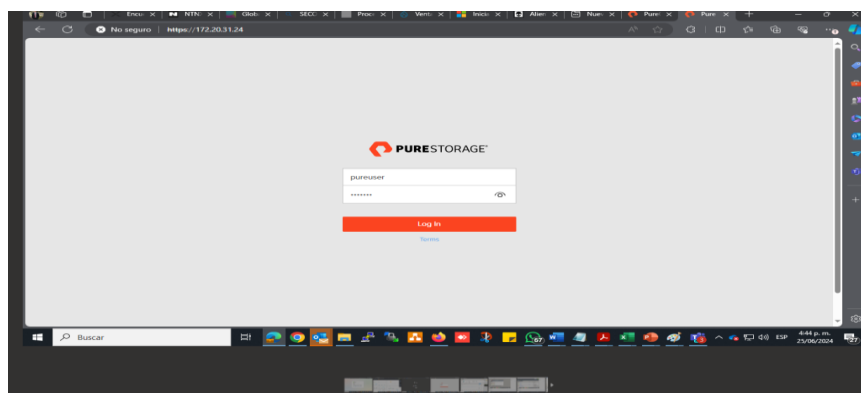
Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 19 de 35

Aplicaciones	Aplicaciones 12H			Aplicaciones 5x12		
	Periodo Indisponibilidad	Horas Indisponibilidad	Total Horas Disponibles	Horas Disp. x mes	Mes	
SICOF	0	0,00	984	252	Enero	21 días hábiles - 2 festivos
PROTOCOLO	0	0,00	984	252	Febrero	21 días hábiles - 0 festivos
CARIBU	0,0	0,00	984	216	Marzo	18 días hábiles - 3 festivos
SIAD	0,0	0,00	984	264	Abril	22 días hábiles - 0 festivos
SISE	0,0	0,00	984			
SIGUEME	0,0	0,00	984			
SINPLE	0,0	0,00	984			
AUSENTISMO LABORAL	0,0	0,00	984			
BIBLIOTECA DE TRATADOS	0,0	0,00	984			
BIBLIOTECA	0,0	0,00	984			
SISTEMA MAESTRO	0,0	0,00	984			
CANDIDATURAS, CUOTAS Y CONTRIBUCIONES - C3	0,0	0,00	984			
COOPERACION JUDICIAL	0,0	0,00	984			
CONSULTA DE CASOS DE DERECHOS HUMANOS	0,0	0,00	984			
INTELIGENCIA DE NEGOCIOS - POWER BI	0,0	0,00	984			
DIRECTORIOS FUNCIONARIOS - MISIONES EN COLOMBIA Y EL INFORME AL CONGRESO	0,0	0,00	984			
INFORME EMBAJADORES	0,0	0,00	984			
PLATAFORMA E-LEARNING	0,0	0,00	984			
PROCESOS DISCIPLINARIOS	0,0	0,00	984			
RECOMENDACIONES DERECHOS HUMANOS	0,0	0,00	984			
CERTIFICACIONES DTH	0,0	0,00	984			
SISTEMA DE REGISTRO Y CONTROL ACADEMIA DIPLOMATICA	0,0	0,00	984			
				984	Total	
		0,00	22632			1440
CALCULO INDICADOR PARA SISTEMA DE CALIDAD						
	HORAS DISPONIBLES	45864				
	TOTAL INDISPONIBIL	101,72				
	INDICADOR	99,77822112				
				% Disponibilidad = ((Horas Disponibles-Horas Indisponibilidad)/Horas Disponibles)*100 % Disponibilidad = ((45864-101,72)/45864)*100 % Disponibilidad = 99,778		

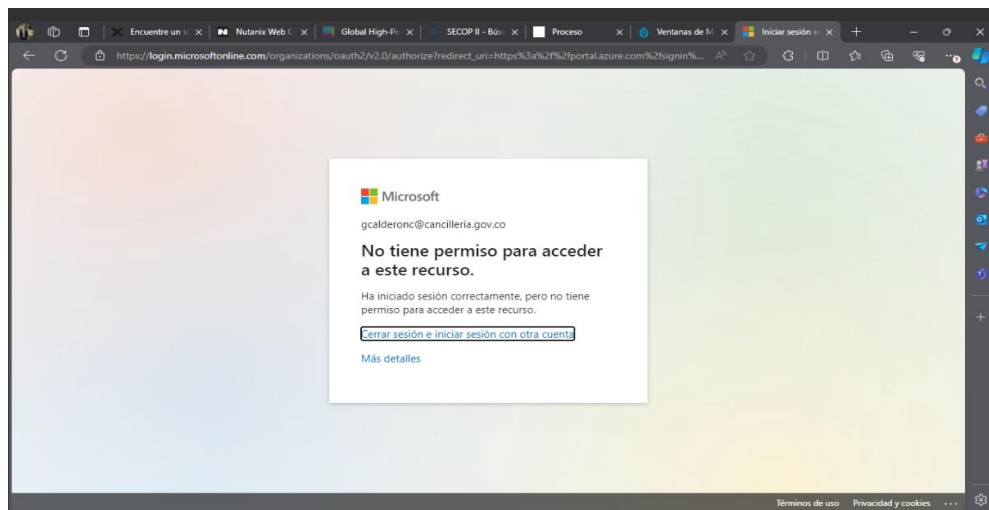
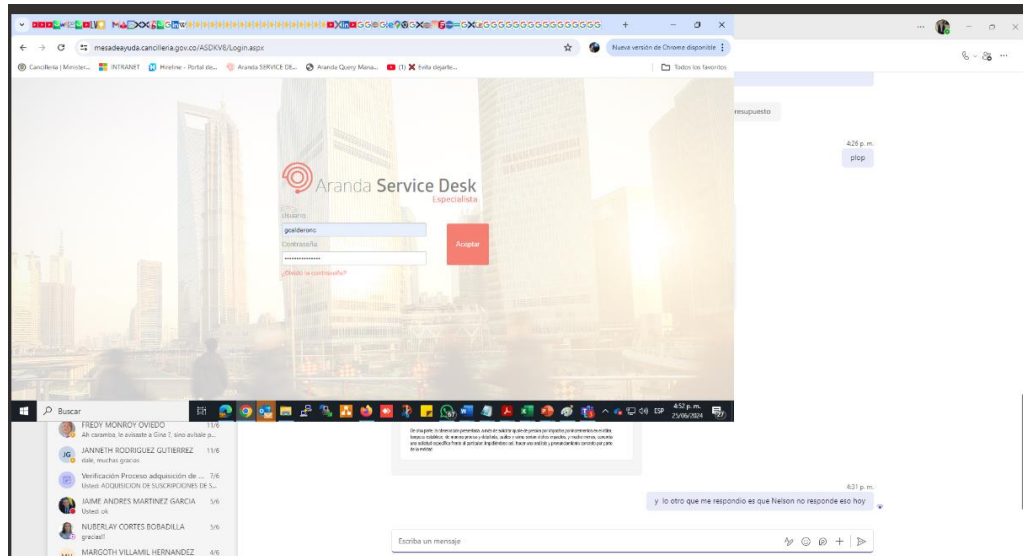
De igual forma se indaga acerca de la confiabilidad de la seguridad de esta información en relación con su acceso, si este es restringido, y quienes tienen acceso a este tipo de información, para lo que el auditado presenta varias herramientas en donde se comprueba que estas no son de acceso para todos los ingenieros de la dirección y que solo unos pocos disponen de estos permisos y tienen dicha responsabilidad para su control y acceso.



Elaboró: Olga Milena Mendoza

FV: 20/05/2020

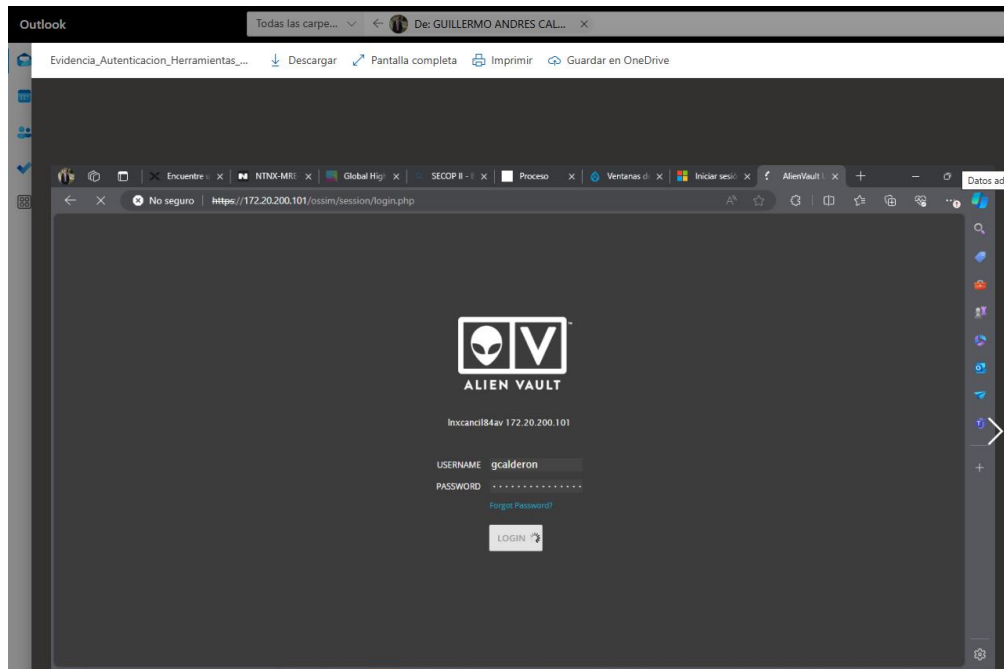
TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 20 de 35



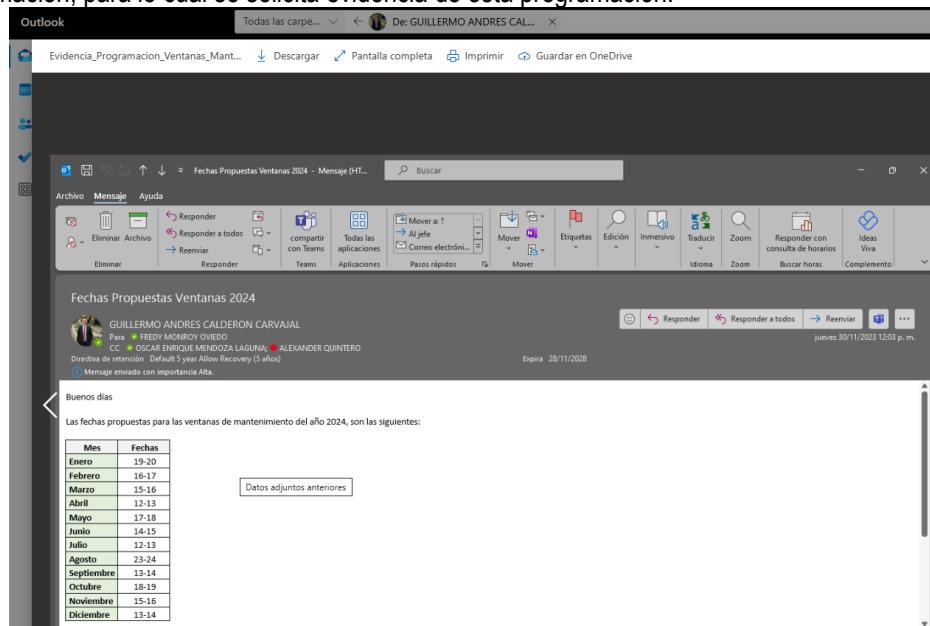
Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 21 de 35



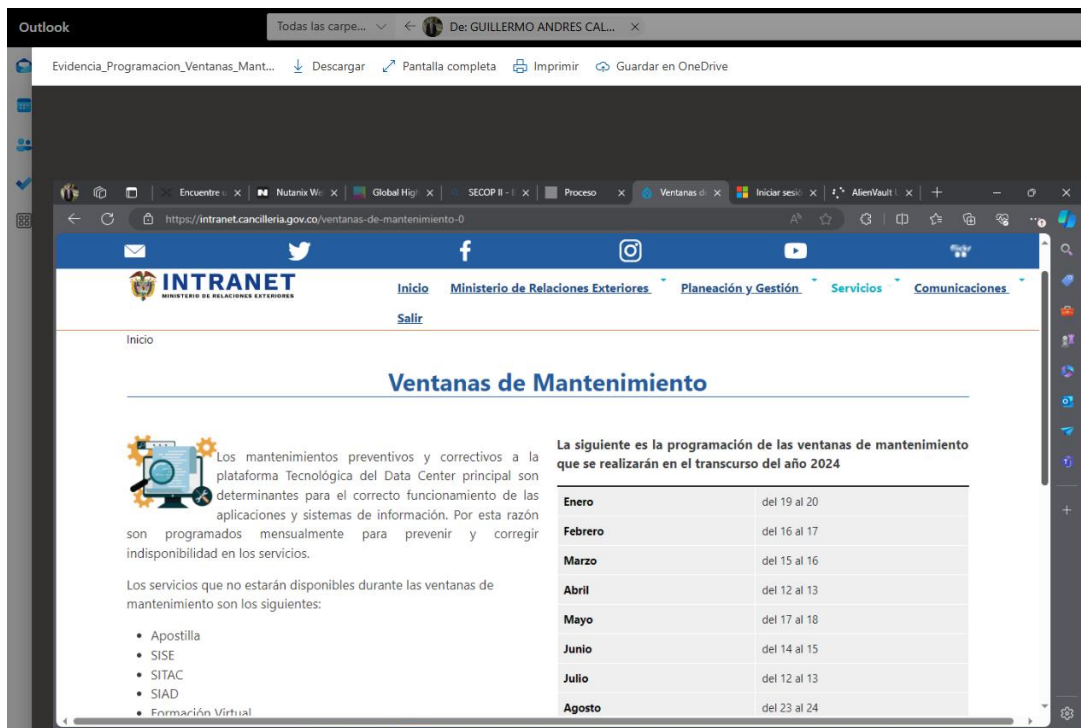
De igual forma se indaga acerca de la programación de las ventanas de mantenimiento, de los diferentes sistemas de información, para lo cual el auditado afirma que estas se realizan de forma programada con el equipo de ingenieros y se realiza su programación, para lo cual se solicita evidencia de esta programación:



Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 22 de 35



The screenshot shows an Outlook email interface. The email content is a webpage from the INTRANET of the Ministry of Foreign Affairs, titled "Ventanas de Mantenimiento". The page features a navigation menu with "Inicio", "Ministerio de Relaciones Exteriores", "Planeación y Gestión", "Servicios", and "Comunicaciones". The main content area includes a heading "Ventanas de Mantenimiento" and a sub-heading "La siguiente es la programación de las ventanas de mantenimiento que se realizarán en el transcurso del año 2024". Below this is a table listing maintenance windows by month and date range.

Month	Period
Enero	del 19 al 20
Febrero	del 16 al 17
Marzo	del 15 al 16
Abril	del 12 al 13
Mayo	del 17 al 18
Junio	del 14 al 15
Julio	del 12 al 13
Agosto	del 23 al 24

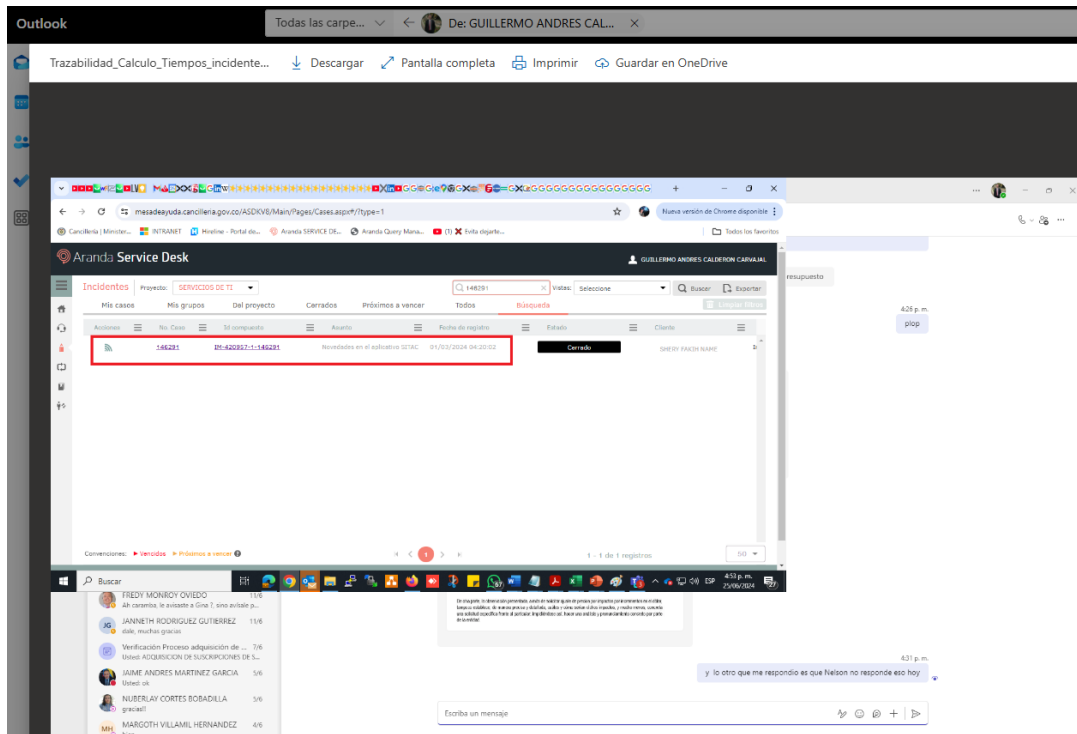
De igual forma el equipo de auditores indaga acerca del tratamiento de incidentes de caídas de aplicativos o falta de los mismos una vez estos son reportados por el usuario de los mismos.

A lo que el auditado explica que lo primero que se hace por parte del usuario del aplicativo es colocar el caso en la herramienta Aranda destinada para estos fines.



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 23 de 35

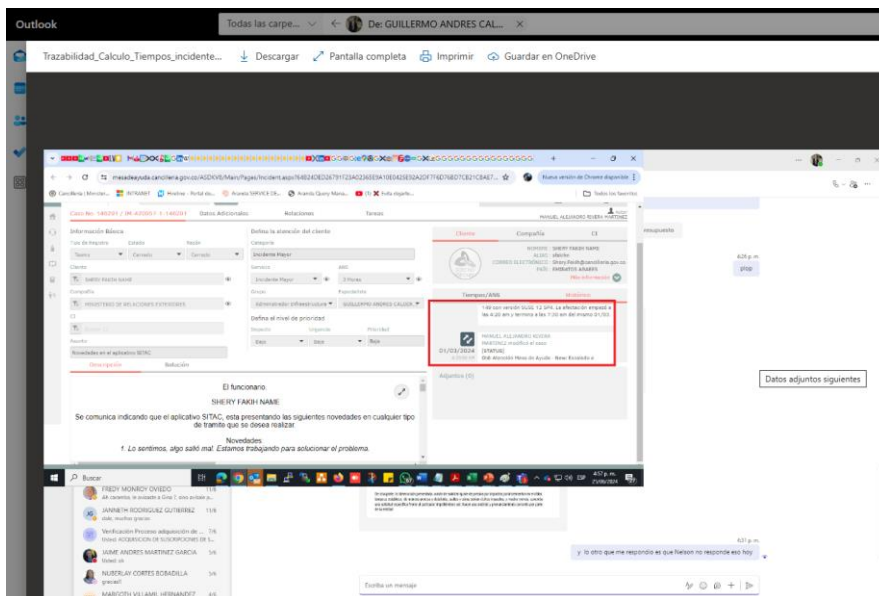


Si el caso se puede solucionar por parte del técnico de mesa de ayuda, este procede a realizarlos en caso contrario procede a escalarlo con los ingenieros responsables del soporte del aplicativo.

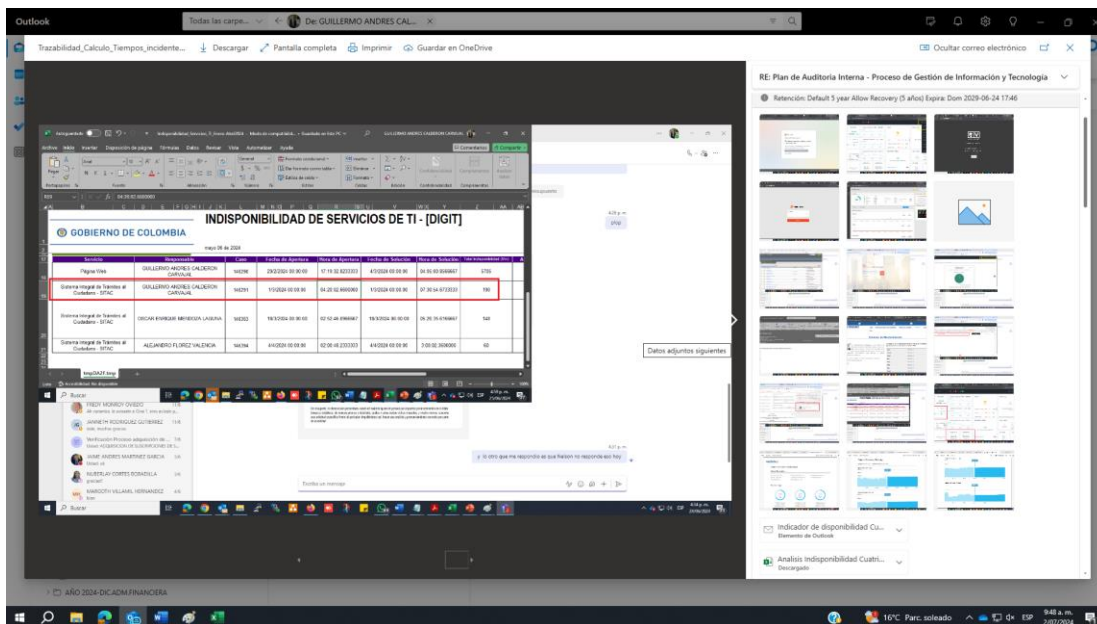
Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 24 de 35



El caso de igual forma queda reportado en la herramienta de indisponibilidad de servicios tecnológicos, para su solución.



Elaboró: Olga Milena Mendoza

FV: 20/05/2020



TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 25 de 35

Como se puede visualizar el equipo de ingenieros encargados del manejo de este tipo de incidente, tiene a su disposición herramienta de control y de manejo a las soluciones de los mismos.

4.8.4 IT-MA-002 V-8 Manual de Seguridad y privacidad de la información v-8

El equipo auditor procede a solicitar información acerca del objetivo y alcance del manual a lo que el auditado denominado oficial de seguridad procede a realizar una descripción de estas ,informando que su objetivo tiene como finalidad dar a conocer lineamientos para velar por el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, legalidad, finalidad, libertad, veracidad, calidad, seguridad, transparencia, acceso y circulación aplicable a la información de la Entidad, y en relación a su alcance afirma que este es de conocimiento y de aplicabilidad por todos los funcionarios, contratistas, pasantes y terceros, que tengan acceso a los activos de información de la entidad.

Se pregunta acerca de la manera como se da a conocer su difusión a los funcionarios de la entidad y el auditado comenta que este se realiza en el proceso de inducción y de reinducción acerca del conocimiento y de la importancia de conocer el manual ya acerca de su responsabilidad de su aplicación.

De igual forma el auditado afirma que a través de los riesgos suscritos por los diferentes procesos también estos son controlados como seguridad y privacidad de la información.

El equipo auditor procede a indagar acerca del manejo que se le da a la materialización de un riesgo que sea de carácter de materialización de privacidad y seguridad de la información, para lo que el auditado informa que una vez se conoce del caso se procede a seguir registrado en mesa de ayuda y se inicia el protocolo de manejo de incidentes.



TIPO DE DOCUMENTO:	FORMATO	CODIGO: CO-FO-05
NOMBRE:	ACTA REUNIÓN / LISTADO DE ASISTENCIA	VERSION: 5
RESPONSABILIDAD POR APLICACIÓN:	TODOS LOS PROCESOS, EMBAJADAS, CONSULADOS Y MISIONES PERMANENTES DE COLOMBIA EN EL EXTERIOR	Página 1 de 3

1. DATOS GENERALES DE LA REUNIÓN					
Asunto o Tema	Asesoría metodológica análisis de causas incidente 146420 Hacked página Cancillería				
Acta de Reunión	X	Listado de Asistencia	X		
Fecha	10/05/2024	Hora Inicio	9:30	Hora Final	10:10
Presencial	No aplica	Virtual:	Microsoft Teams		
Responsable:	Andrea del Pilar Roza Castro				

Elaboró: Olga Milena Mendoza

FV: 20/05/2020



TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 26 de 35

2. DESARROLLO DE LA REUNIÓN

A través de la presente mesa de trabajo se lleva a cabo el acompañamiento metodológico orientado a la elaboración del análisis de causas en atención al hallazgo:

*Incidente 146420 Hackeo página Cancillería
Incidente reportado el 09 de abril de 2024 por Colcert (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) el cual identifica el ataque de un hacker a las páginas "Patrimonio Arqueológico" y "Gabo 40 aniversario" entre el 30 y 31 de enero de 2024.*

Una vez aplicada la metodología de los 5 por qué's se establecen que las causas que dieron lugar al incidente corresponden a dos de las causas raíz identificadas en el incidente "145830 BITACORA SAN CARLOS":

¿POR QUÉ?	¿POR QUÉ?	¿POR QUÉ?	¿POR QUÉ?	¿POR QUÉ?
El servicio salió a producción sin antivirus Microsoft Defender instalado	Incumplimiento del lineamiento 8.9.5 Protección contra código malicioso establecido en el Manual de Seguridad de la Información IT-MA-002	No existe una línea base de seguridad para los servidores en el procedimiento operativo correspondiente.	No aplica	No aplica

La IP de los sitios publicados no aparecía en el inventario de IP que administra la Oficial de Seguridad de la Información	Incumplimiento IT-IN-004 Gestión de Vulnerabilidades en la política relacionada con el inventario de equipos de comunicaciones, servidores y sistemas de información	No se encuentra un lineamiento operativo respecto al inventario de IP que administra la Oficial de Seguridad de la Información en los procedimientos IT-PT-004 Gestión de Sistemas de Información y IT-PT-009 Gestión de Configuración y Activos de los Servicios de TI	No aplica	No aplica
--	--	---	-----------	-----------

En concordancia a los lineamientos establecidos en el procedimiento MC-PT-010 Identificación, implementación y seguimiento de acciones de corrección, correctivas y de mejora para el tratamiento de no conformidades similares y dado que este incidente comparte dos de las tres causas identificadas en el incidente "145830 BITACORA SAN CARLOS", su tratamiento se realizará a través de las acciones correctivas formuladas para dicho incidente, instrumento que se encuentra en trámite de ajuste y aprobación de la Dirección de Gestión de Información y Tecnología.

Elaboró: Gustavo Alba Castro

FV: 04/08/2021

Elaboró: Olga Milena Mendoza

FV: 20/05/2020



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 27 de 35

No conformidad	Incidentes	<p>Incidente Bitácora de San Carlos</p> <p>Incidente presentado por el ataque de un hacker al servidor de la Bitácora de San Carlos presentado el 03 de noviembre de 2023 e informado al Ministerio de Relaciones Exteriores por la Presidencia de la República donde se presentaba un mensaje de alerta avisando el ataque al ingresar a la URL https://bitacoradesancarlos.cancilleria.gov.co/public/site/images/org0n/org0n.jpg</p>	No existe una línea base de seguridad para los servidores en el procedimiento operativo correspondiente.	Acción Correctiva	Crear una guía en el Sistema Integrado de Gestión que establezca la línea base de seguridad para los servidores de la infraestructura tecnológica del Ministerio de Relaciones Exteriores.
				Acción Correctiva	Formalizar la guía en la cual se establezca la línea base de seguridad para los servidores de la infraestructura tecnológica en el aplicativo del Sistema Integrado de Gestión del Ministerio de Relaciones Exteriores.
				Acción Correctiva	Socializar a los responsables de aplicabilidad la guía que establezca la línea base de seguridad para los servidores de la infraestructura tecnológica del Ministerio de Relaciones Exteriores.
				Acción Correctiva	Implementar la guía que establezca la línea base de seguridad para los servidores de la infraestructura tecnológica del Ministerio de Relaciones Exteriores.
				Acción Correctiva	Definir el lineamiento operativo respecto al inventario de IP que administra la Oficial de Seguridad de la Información en los procedimientos IT-PT-004 Gestión de Sistemas de Información y IT-PT-009 Gestión de Configuración y Activos de los Servicios de TI.

De igual forma se canaliza el incidente con la oficina Asesora de Planeación y Desarrollo organizacional, en el análisis de causas.

Elaboró: Olga Milena Mendoza

FV: 20/05/2020



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 28 de 35



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CODIGO: MC-FO-022
NOMBRE:	ANALISIS DE CAUSAS	VERSIÓN: 6
RESPONSABILIDAD POR APLICACIÓN:	TODOS LOS PROCESOS, EMBAJADAS, CONSULADOS Y MISIONES DE COLOMBIA EN EL EXTERIOR	Página 1 de 3

Fecha de Diligenciamiento	Día	05	Mes	02	Año	2024
---------------------------	-----	----	-----	----	-----	------

	NOMBRE	CARGO / ÁREA	FIRMA
	Hilda Lucy Pabón Benites	Asesora Oficial de Seguridad de la Información Dirección de Gestión de Información y	Documento digital

EQUIPO DE MEJORAMIENTO	NOMBRE	CARGO / ÁREA	FIRMA
	Fredy Monroy Oviedo	Coordinador de GIT de Servicios Tecnológicos Dirección de Gestión de Información y Tecnología	Documento digital
	Alejandro Florez Valencia	Asesor GIT de Servicios Tecnológicos Dirección de Gestión de Información y Tecnología	Documento digital
	Alvaro Enrique Cárdenas	Asesor GIT de Gobierno de TI	Documento digital
	Claudia Mercedes Forero Arias	Asesora GIT de Gobierno de TI	Documento digital

DESCRIPCIÓN DE LA NO CONFORMIDAD

Incidente Bitácora de San Carlos

Incidente presentado por el ataque de un hacker al servidor de la Bitácora de San Carlos presentado el 03 de noviembre de 2023 e informado al Ministerio de Relaciones Exteriores por la Presidencia de la República donde se presentaba un mensaje de alerta avisando el ataque al ingresar a la URL

<https://bitacoradesancarlos.cancilleria.gov.co/public/site/images/org0n/org0n.jpg>

Elaboró: Olga Milena Mendoza

FV: 20/05/2020

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 29 de 35

Es de anotar que una vez realizado este análisis se procede a suscribir plan de mejoramiento para manejo del mismo para su solución final.

Todo incidente conlleva a los siguientes documentos de soporte de su registro y control:

Evidencias de la gestión de incidentes:

Incidentes 145830 Bitácora de San Carlos y 146420 Hackeo página web

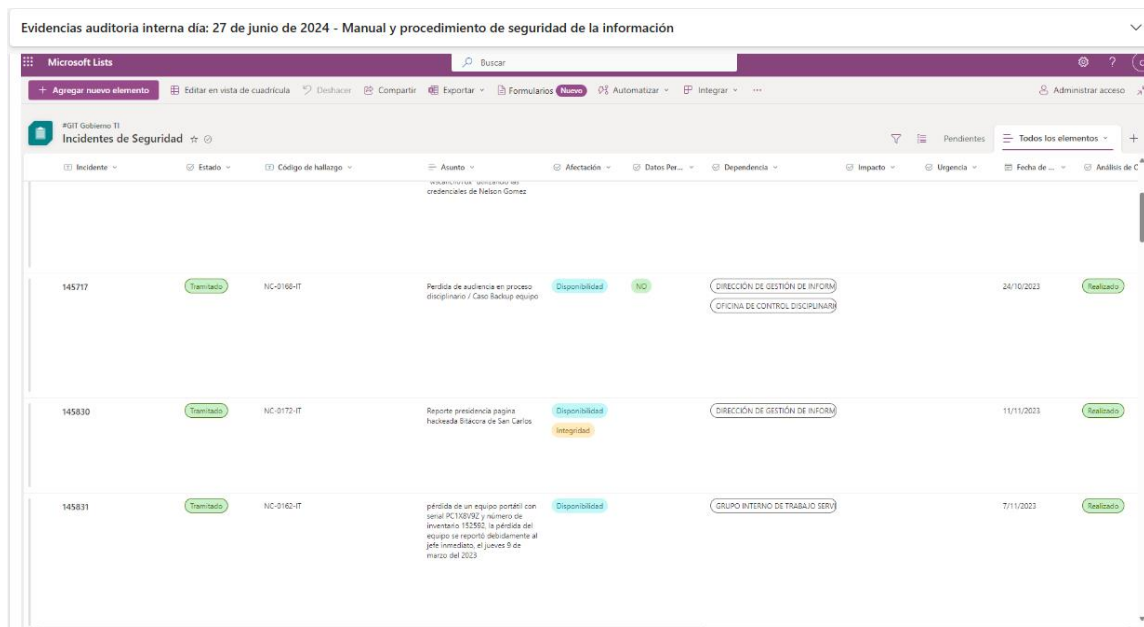
Para consultar el plan de mejoramiento en la SVE, indicar el código de hallazgo: NC-0172-IT

Acta de reunión equipo de incidentes casos - 2024-05-10 Acta de reunión PMP incidente 146420 Hackeo página Cancillería

Análisis de causas: 2024-02-05 MC-FO-022 Análisis de Causas San Carlos DIGIT (1)

Análisis de causas: 2024-05-10 MC-FO-022 Análisis de Causas Hackeo página Cancillería

Imagen de la relación de incidentes para su gestión en Microsoft List:



Incidente	Estado	Código de hallazgo	Asunto	Afectación	Datos Per...	Dependencia	Impacto	Urgencia	Fecha de ...	Análisis de C
145717	Tramitado	NC-0168-IT	Perdida de credenciales de Nelson Gomez	Disponibilidad	NO	DIRECCION DE GESTIÓN DE INFORMACIÓN OFICINA DE CONTROL DISCIPLINAR			24/10/2023	Realizado
145830	Tramitado	NC-0173-IT	Reporte presidencia pagina Hackeada Bitacora de San Carlos	Disponibilidad	Integridad	DIRECCION DE GESTIÓN DE INFORMACIÓN			11/11/2023	Realizado
145831	Tramitado	NC-0162-IT	pérdida de un equipo portátil con serial PC1X0292 y número de inventario 132582 la pérdida del equipo se reportó debidamente al jefe inmediato el jueves 9 de mayo del 2023	Disponibilidad		GRUPO INTERNO DE TRABAJO SERVI			7/11/2023	Realizado

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 30 de 35

Al indagar acerca del manejo de la matriz que se maneja para establecer su impacto, los auditados informan que se basan en una matriz ya establecida para tal fin.

Evidencias auditoria interna día: 27 de junio de 2024 - Manual y procedimiento de seguridad de la información

- Imagen de la Guía de Activos de la información IT-GS-005 - matriz de impacto



TIPO DE DOCUMENTO:	GUÍA	CÓDIGO: IT-GS-05
NOMBRE:	GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN	VERSIÓN: 1
RESPONSABILIDAD POR APLICACIÓN:	TODOS LOS PROCESOS, EMBAJADAS Y CONSULADOS DE COLOMBIA EN EL EXTERIOR	Página 10 de 12

8.6.3. De acuerdo con la Disponibilidad

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

Disponibilidad	Descripción
Alta (1)	La pérdida de disponibilidad puede conllevar un impacto negativo de índole legal o económica o generar pérdidas de imagen severas a Terceros. (Ej: Procuraduría, Defensoría del Pueblo, Contraloría, Ministerios, Fiscalía, entre otros)
Media (2)	La pérdida de disponibilidad puede conllevar un impacto negativo de índole legal o económica o generar pérdidas de imagen moderada a los procesos internos de la Entidad
Baja (3)	La pérdida de disponibilidad puede generar un impacto no significativo a nivel interno del proceso
No Clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA .

Tabla 5: Criterios de disponibilidad de la información

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 31 de 35

Evidencias auditoria interna día: 27 de junio de 2024 - Manual y procedimiento de seguridad de la información

No Clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA .
-----------------------	--

Tabla 5: Criterios de disponibilidad de la información

8.6.4. Criticidad

Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la información realizada en los pasos anteriores.

- Alta: Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
- Media: Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio.
- Baja: Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

- Actualización parches de seguridad - ventana de mantenimiento de mayo 2024

De: ALEJANDRO FLOREZ VALENCIA <alejandro.florez@cancilleria.gov.co>

Enviado: lunes, 6 de mayo de 2024 10:24 a. m.

Para: CLAUDIA MERCEDES FORERO ARIAS <claudia.forero@cancilleria.gov.co>; FREDY MONROY OVIEDO <Fredy.Monroy@cancilleria.gov.co>

Cc: DORA STELLA AMADO HERNANDEZ <dora.amado@cancilleria.gov.co>

Asunto: RE: 🚨 Solicitud evidencias: Mapa de Riesgos I trimestre 2024

Buenos días Claudia,

A continuación, las evidencias del despliegue de parches de la última ventana:

WinSrv2016 Monthly Updates 2024-04-10 19:01:41 Status to Windows Server 2016

Es de aclarar que la aplicación de este análisis del impacto del incidente no queda clasificado de forma clara en el acta de reunión para el tratamiento del caso, por parte de los ingenieros de sistemas como lo indica el procedimiento, lo que para el equipo auditor no es claro en su clasificación o categorización.

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 32 de 35

4.9. TABLA DE RETENCIÓN DOCUMENTAL DE LA DIRECCIÓN GD-FO-03 Versión 10 vigente

Manual de archivo GD- MA -03 describe la forma de marcar y archivar documentos de la siguiente manera:

El Manual de archivo GD- MA -03 vigente, establece en su artículo 8.2.3 GESTIÓN Y TRÁMITE:

Se registra el número consecutivo con el que se identifica cada una de las carpetas en el inventario del Archivo de Gestión o para la transferencia primaria.

La rotulación de las carpetas debe ser realizada de acuerdo con la Tabla de Retención Documental vigente, que se encuentra publicada en la página web de la Cancillería: https://www.cancilleria.gov.co/ministry/strategy/document_management/documentary_withholding_tables

Las carpetas que contienen documentos hasta diciembre de 2017 deben estar identificadas con los códigos y los nombres correspondientes a la Tabla de Retención Documental anterior.

En relación con la clasificación de los documentos dentro de la carpeta el procedimiento dice textualmente: “En cada carpeta, los documentos deben estar ordenados cronológicamente de manera que se pueda evidenciar el desarrollo de los trámites, del más antiguo al más reciente, en forma de libro”.

Por evidencia el equipo auditor reviso 5 carpetas de la Dirección, donde identificó que 3 no cumplían con lo anteriormente mencionado.

MINISTERIO DE RELACIONES EXTERIORES	
CÓDIGO DE LA SERIE: 20.79	
OFICINA PRODUCTORA: GRUPO INTERNO DE TRABAJO DE CEREMONIAL DIPLOMÁTICO	
SERIE: CONDECORACIONES	
SUBSERIE: CONDECORACIONES NACIONALES ORDEN DE BOYACÁ	
TÍTULO DE LA CARPETA: ORDEN DE BOYACÁ 2019	
FOLIOS: 56	Nº CORRELATIVO 1 DE 2
FECHAS EXTREMAS: ENERO 2019 A JULIO 2019	
CAJA Nº 69975	CARPETA Nº 2

Ilustración

1 Ejemplo diligenciamiento de rótulo para identificar carpetas

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 33 de 35

5.0. FORTALEZAS

- Cumplimiento de los objetivos estratégicos de la Entidad y la implementación del Sistema Integrado de Gestión en cada uno de los procesos.
- Se resalta el alto compromiso institucional de cada uno de los líderes de la Dirección y sus Grupos de Trabajo, que se reflejan en el cumplimiento de los lineamientos establecidos por la entidad para garantizar que los procesos se desarrollen de forma efectiva, eficiente y eficaz.
- Se resalta el conocimiento de cada uno de los coordinadores de la dirección y de sus equipos de trabajo respecto a sus actividades en el marco del Sistema Integrado de Gestión.
- Se destaca el trabajo, el conocimiento y el aporte a la gestión de la dirección por parte de la gestora de cambio del proceso.
- Se reconoce el manejo eficiente y documentado de las actividades adscritas al proceso de Gestión de información y tecnología, esto con el fin de mantener la trazabilidad de la gestión para cualquier ente de control o funcionario de la entidad, o de la dirección, que lo llegue a requerir.

6.0. OPORTUNIDADES DE MEJORA

- Fortalecer el seguimiento periódico a la ejecución del plan de adquisiciones, que va de la mano con la ejecución presupuestal, con el fin de garantizar su cumplimiento y evitar que se repita lo sucedido con la ejecución presupuestal del 2023.
- Realizar seguimiento a los informes de la Oficina de Control Disciplinario Interno acerca de los casos reportados respecto a las vulnerabilidades de los sistemas de información o casos de incidentes de seguridad, con el fin de validarlos frente a los identificados y notificados a la Dirección de Gestión de Información y Tecnología.
- Evaluar la pertinencia de eliminar o actualizar de forma permanente lo relacionado con la telefonía IP en la Cancillería.
- Revisar en detalle y atender las observaciones realizadas por los GIT de Control Interno de Gestión, y Gestión y Desempeño Institucional, producto de los reportes de seguimiento al Mapa de Riesgos Integrado.

7.0. NO CONFORMIDAD

ITEM	CRITERIO DE AUDITORIA O NORMA	DESCRIPCIÓN
1	8.1 ISO 14001	En el recorrido por las oficinas de la Dirección para la revisión del cumplimiento de separación de residuos, se evidenció que en papeleras ubicadas en los puestos de trabajo se desechan residuos aprovechables como el papel de reciclaje y botellas de plástico, revueltos con desechos no aprovechables, incumpliendo así lo establecido en el programa "Gestión integral de residuos sólidos" AS-PG-003 en su versión 4, específicamente en lo relacionado con el numeral 7.2.4. Manejo de los residuos "Además de los puntos ecológicos, todas las dependencias cuentan con una papelería sin rotulo por cubículo; donde son depositados los residuos no aprovechables".

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 34 de 35

2	Manual de archivo GD-MA -03. 7.5.3 2 a ISO 9001	Se evidenció que dos carpetas de manejo documental de la dirección no estaban marcadas con su respectivo rotulo según la tabla de retención documental vigente y los registros archivados en ellas no se encuentran en orden cronológico de lo mas nuevo a lo más antiguo incumplimiento de lo establecido en el Manual de archivo GD- MA -03. en su artículo 8.2.3 GESTIÓN Y TRÁMITE, con relación a la forma de marcación y archivo de documentos generados en la entidad.
3	IT-PT-023 Manejo de incidentes de seguridad y privacidad de la información con o sin afectación de datos personales	Para los incidentes 145830 Bitácora de San Carlos, y 146420 hackeo página, se realizaron reuniones con actas de reunión 2024-02-05 y 2024-05-10, con el fin de determinar las acciones a realizar respecto a cada incidente sin que se evidencie el análisis del impacto para la definición del nivel de urgencia de estos, incumpliendo lo establecido en el procedimiento IT-PT-023 Manejo de incidentes de seguridad y privacidad de la información con o sin afectación de datos personales, en su versión 2, en la política "8.4. Evaluación, "El Equipo de Respuesta a Incidentes establecerá el impacto, la urgencia que el incidente puede generar a la entidad, dependiendo de cómo éste afecta los procesos misionales, cantidad de activos de información afectados, usuarios afectados y la criticidad.

8.0. CONCLUSIONES DEL INFORME

Se concluye que el proceso de Gestión de Información y Tecnología es adecuado y conveniente para el cumplimiento de los requisitos de las normas NTC ISO 9001:2015 & 14001:2015 y el proceso evidencia el cumplimiento de su objetivo.

Tanto para los hallazgos como para las oportunidades de mejora identificadas se hace necesario la definición e implementación de Planes de Mejoramiento a partir de los resultados presentados anteriormente, esto con el fin de fortalecer la implementación del Sistema Integrado de Gestión.

Equipo auditor:

Documento Electrónico
César Augusto Cufiño Cufiño
Asesor
Auditor Líder

Elaboró: Olga Milena Mendoza

FV: 20/05/2020



Libertad y Orden

TIPO DE DOCUMENTO:	FORMATO	CÓDIGO: EI-FO-09
NOMBRE:	INFORME DE EVALUACIÓN	VERSIÓN: 4
RESPONSABILIDAD POR APLICACIÓN:	GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO DE GESTIÓN, ÁREAS RESPONSABLES DE LOS SISTEMAS DE GESTIÓN IMPLEMENTADOS EN EL MINISTERIO DE RELACIONES EXTERIORES Y SU FONDO ROTATORIO - AUDITORES INTERNOS	PÁGINA: 35 de 35

Documento Electrónico

Johany Marleny Mesa Rodríguez

Asesora

Auditor Acompañante

Documento Electrónico

Jenny Andrea Hernández Alfonso

Coordinadora GIT Gestión y Desempeño Institucional

Elaboró: Olga Milena Mendoza

FV: 20/05/2020