ID	Planes de tratamiento
PT029	Contratar un tercero para la ejecución de auditorias periódicas al sistema de gestión de seguridad de la información, que incluyan la verificación del cumplimiento del numeral 7.2 del estándar 27001:2013 sobre la competencia de las personas que realizan un trabajo que afecte el desempeño de la seguridad de la información.
PT008	Implementar o contratar a un tercero para hacer la remediación de las vulnerabilidades identificadas en los análisis trimestrales. Las vulnerabilidades se deben cerrar de acuerdo a la criticidad de la misma, iniciando por las más críticas y debe respetar el procedimiento de control de cambios definido en el INS.
PT026	Contratar un tercero especializado en el diseño e implementación de capacitaciones sobre la importancia del cumplimiento de las políticas y procedimientos de seguridad definidos y aprobados en el INS, con su correspondiente evaluación del conocimiento entregado, para identificar oportunidades de mejora que garanticen que los funcionarios y contratistas aplican la seguridad de la información en el día a día. Los referentes de proceso deberán recoger los resultados de las evaluaciones y realizar retroalimentación personalizada a las personas de sus correspondientes procesos.
PT022	Fortalecer los controles de acceso para visitantes y contratistas que incluyan: una identificación adecuada y garantizar el acompañamiento cuando estos accedan a zonas seguras. Para los archivos físicos, los referentes de proceso deberán realizar una verificación semanal de las condiciones ambientales de la zona donde están instalados, detectando condiciones ambientales que puedan afectar los activos de información: humedad, inundación, fuego, temperaturas elevadas, contaminación. Como parte de la verificiación, el referente deberá proponer un plan de acción para evitar que se deterioren (o se amplie el deterioro) de la información.

PT048	Contratar una auditoria externa para que verifique trimestralmente que el Datacenter del INS cumple con las buenas practicas en cuanto al mantenimiento y administración de este tipo de instalaciones. La auditoría debe incluir al menos la revisión de: - Controles de acceso físico - Bitácoras de registro - Circuito cerrado de televisión y grabación de video - Suelo y techo falso - Seguridad del cableado - Detección y extinsión de incendios - Mantenimiento - Respaldo eléctrico
PT038	Garantizar que la seguridad de la información se incluye como parte de la arquitectura empresarial del INS. El área de planeación será responsable por garantizar que la seguridad de la información sea parte del proyecto de arquitectura.
PT030	Contratar un tercero para diseñar y hacer el acompañamiento en la implementación y pruebas periódicas a un plan de continuidad de negocio, en el que contemplen instalaciones físicas, procesos de negocio y la plataforma tecnológica del INS. Los referentes de proceso deberán participar activamente en el diseño del plan y serán responsables por las pruebas y mejora continua del plan de sus respectivos procesos.

PT015	Contratar la adquisición, configuración e implementación de una solución DLP (Data Loss Prevention) que permita monitorear y/o bloquear la salida de información por puertos USB de los computadores y/o servidores, por correo electrónico y por servicios de red (incluido Internet). Los permisos y excepciones dependerán del nivel de confidencialidad de los activos de información, en concordancia con la política de medios removibles establecida en el manual de políticas de seguridad de la información. Los referentes del proceso deberán garantizar que sus activos de información estén correctamente actualizados y cladificado, y deberán verificar periódicamente que las reglas configuradas son efectivas (por ejemplo intentar copiar un archivo a una USB y confirmar que no es posible)
PT004	Habilitar los registros de las acciones ejecutadas por usuarios con perfil de administrador y otros usuarios en la plataforma critica del INS, los cuales deben ser enviados a un correlacionador de eventos (SIEM) contratado como servicio. Los referentes de proceso deben garantizar que la habilitación de la auditoría (logs) se implemente para los sistemas de información o aplicaciones desarrolladas o implementadas en el proceso, informando al área OTIC para que se recolecte la información en el SIEM.
PT010	Contratar el servicio de verificación de cumplimiento de las guías de aseguramiento o hardening para los sistemas de información, elaborando planes de acción cuando se encuentren desviaciones. Los referentes de proceso deben realizar seguimiento a los correspondientes planes de acción para garantizar que estos se implementran según lo definido.
PT036	Contratar un servicio de aseguramiento o hardening de los sistemas de información y plataformas criticas, siguiendo buenas prácticas como NIST o CIS. El aseguramiento debe definir guías de hardening que incuyan los controles más importantes dependiendo del software (sistemas operativos, motores de bases de datos, servidores web, etc.), incluyendo la desactivación de los usuarios administradores que vienen de fábrica en dichas plataformas. Los referentes de proceso deben garantizar semestralmente que la infraestructura que soporta los sistemas de información o aplicaciones de su servicio se encuentran debidamente asegurados.
PT009	Contratar un tercero para efectuar Ethical hacking semestral a los sistemas de información y las aplicaciones mas criticas del INS. Los referentes del proceso deben garantizar que los activos de información más críticos estén incluidos en el ethical hacking.

PT012	Implementar una única política para el uso de contraseñas fuertes por parte de los funcionarios y contratistas del INS. La política de contraseña debe incluir logitud mínima, edad mínima, solicitar complejidad (mínimo una mayúscula, una minúscula, un número y un simbolo), almacenamiento cifrado y tener un histórico de contraseñas que no se puedan utilizar. Los referentes de proceso deberán garantizar que esta política se implemente para los sistemas de información o aplicaciones desarrolladas o implementadas en el proceso.
PT028	Generar capacitaciones de reinducción anuales que se centren en la importancia de los sistemas de gestión, sus políticas y procedimientos asociados, la importancia de su cumplimiento y los resultados obtenidos con su implementación. Los referentes de proceso deberán garantizar que personal de planta y contratistas de sus procesos estén debidamente capacitados.
PT050	Contratar un servicio de alertas tempranas o vulnerabilidades de día cero que permita identificar y gestionar las vulnerabilidades más recientes. Los referentes del proceso deben verificar periódicamente que las alertas tempranas se gestionen hasta su cierre.
PT006	Contratar una consultoría para el diseño y acompañamiento en la implementación de una metodología de desarrollo seguro basado en los principios y buenas practicas definidas por el Open Web Aplicación Security Project (OWASP). Los referentes de proceso deben garantizar la participación de los desarrolladores de las aplicaciones de sus procesos en el diseño e implementación de dicha metodología.
PT005	Contratar un servicio SOC o CSIRT para la gestión de incidentes de seguridad de la información y ciberseguridad en modalidad 7x24. El servicio deberá realizar la detección de todos los incidentes registrados en el SIEM, indicando las medidas de contención a seguir para evitar que el incidente continue o se incremente su impacto. Los referentes de proceso deberán hacer parte de la gestión del incidente cuando se presenten en los sistemas de información o aplicaciones desarrolladas o implementadas en el proceso, haciendo parte de la matriz de escalamiento del incidente.

PT031	Contratar la revisión periódica del cableado eléctrico de instalaciones criticas, como: centros de computo, laboratorios, etc., identificando los planes de acción que sean aplicables. Los referentes de proceso deberán acompañar las revisiones y serán responsables por la implementación de los planes de acción definidos.
PT047	Adquirir una solución de IDS/IPS para la detección y prevención oportuna de intrusos a la plataforma tecnológica del INS. Una vez implementado, los referentes del proceso deben verificar trimestralmente que los activos de información más críticos están configurados en la solución IDS/IPS.
PT046	Realizar pruebas de restauración (al menos mensualmente) de backups o copias de respaldo para garantizar que la información se podrá recuperar en caso de ser necesario. Los referentes de proceso serán responsables por solicitar y/o coordinar las pruebas de restauración y verificar sus resultados.
PT039	Adquirir una solución que permita el cifrado de computadores con información sensible, dispositivos móviles y unidades de almacenamiento removibles, como: portátiles, tablets, discos duros externos, memorias USB que son retirados del INS por motivos laborales con el fin de prevenir el acceso no autorizado a dicha información en caso de perdida. Los referentes de proceso son los responsables por contar con un inventario actualizado de estos dispositivos y garantizar que están debidamente cifrados.
PT021	Contratar un tercero para que realice la auditoria semestal del servicio prestado por la empresa de seguridad física, con el fin de identificar fallas en los controles de acceso y proponer mejoras que fortalezcan la seguridad física del INS y por ende de los activos de información que se almacenan física o lógicammente dentros del instituto. El tercero debe realizar como parte de la auditoría un análisis de riesgos de seguridad física, incluyendo los aspectos ambientales (inundación, fuego, terremotos, etc.), proponiendo los correspondientes planes de tratamiento.

PT011	Contratar un tercero para la adquisición, configuración e implementación de una solución WAF que permita monitorear y prevenir ataques hacia las aplicaciones web criticas que tiene el INS. Los referentes de proceso participarán y garantizarán que se han configurado reglas de protección para los sistemas de información y/o aplicaciones desarrolladas o implementadas en sus procesos.
PT003	Adquirir una solución de File Integrity Monitoring (FIM) o contratarlo como servicio, que permita el monitoreo de cualquier modificación no autorizada en activos de información críticos. Los referentes del proceso deben garantizar que los activos de información más críticos estén incluidos en el monitoreo de integridad, teniendo en cuenta la criticidad de los activos de información.
PT007	Contratar el análisis de vulnerabilidades trimestrales a los sistemas de información y aplicaciones mas criticas del INS. Los referentes del proceso deben garantizar que se ejecutan los escaneos, conociendo y gestionando el correspondiente plan de cierre o mitigación de vulnerabilidades.
PT034	Contar con un stock de partes susceptibles de falla de la infraestructura critica con el fin de reemplazarlas en el menor tiempo posible.
PT019	Garantizar que la infraestructura tecnológica que se encuentra presente en los Centros de Computo, como: servidores, switches, appliances, cuenten con contrato de mantenimiento preventivo y correctivoperiódico, verificando que este se ejecuta de acuerdo a lo contratado.
PT002	Verificar que la solución de antivirus cuente con políticas para garantizar que todo archivo descargado sea analizado inmediatamente en busca de malware, y eliminando en caso de estar infectado. Los referentes del proceso deben verificar semanalmente que los equipos tienen el antivirus actualizado. La verificación se debe realizar en el 10% de los computadores del proceso, probando la semana siguiente otro 10% hasta cubrir el 100% de los equipos, volviendo a inicar el ejercicio.

PT032	Llevar un control de usuarios y perfiles con acceso a los activos de información, garantizando que solo acceden exclusivamente a lo necesario, teniendo en cuenta los roles y funciones desempeñados. Los referentes de proceso deberán garantizar mensualmente que los usuarios y perfiles son los correctos, solicitando las novedades (retiro o modificación) que sean necesarias en caso de encontrar desviaciones.
PT035	Contratar un tercero especialista en diseño, análisis e implementación de planes de capacidad, los cuales deben incluir al menos las variables de almacenamiento, procesamiento y transmisión. Los referentes de proceso deben garantizar que se ejecuta el plan de capacidad para la infraestructura que soporta los sistemas de información o aplicaciones de su proceso.
PT044	Adquirir o contratar una solución de de protección de amenazas avanzadas en correo electrónico, incluyendo protección para phishing, spear phishing, APT, scam y otras técnicas de ataque.
PT013	Realizar campañas de concienciación sobre el bloqueo de la pantalla por parte de funcionarios y contratistas al momento de retirarse del puesto de trabajo. Los referentes del proceso deben verificar todos los días que los usuarios realicen el bloqueo antes de levantarse del puesto. En caso de encontrar puestos abandonados con la sesión abierta, deberán realizar la retroalimentación correspondiente para que la situación no vuelva a ocurrir.
PT014	Realizar campañas de concienciación sobre el uso adecuado de contraseñas: No compartir, no anotar en post-it, no anotar en archivos digitales en texto claro. Los referentes del proceso deben verificar todos los días que los usuarios no escriban contraseñas. En caso de evidenciar esta mala práctica, deberán realizar la retroalimentación correspondiente a los usuarios para que se cambie de inmediato la contraseña, haciendo enfasis en que no debe volver a ocurrir.

PT027	Asegurar que se realicen inducciones que incluyan a funcionarios y contratistas nuevos para garantizar que conozcan la entidad, los objetivos y procesos del negocio, así como los diferentes sistemas de gestión, sus políticas y procedimientos asociados y la importancia de su cumplimiento. Los referentes de proceso deberán garantizar que personal de planta y contratistas de sus procesos estén debidamente capacitados.
PT033	Renovar la infraestructura critica que soporta sistemas de información y servicios de TI críticos que no cuenten con soporte por obsolescencia tecnológica.
PT017	Garantizar el mantenimiento y pruebas de funcionamiento trimestrales de los elementos de control ambiental vitales para el DataCenter como son: aires acondicionados, sistema contraincendios, UPS y plantas eléctricas.
PT018	Contratar una solución que permita monitorear y alertar sobre cambios en las condiciones ambientales del DataCenter, generando las alarmas que sean necesarias para actuar de manera ágil ante variaciones que puedan afectar el desempeños de la infraestructura tecnológica.
PT001	Crear una lista blanca de las extensiones (por ejemplo PDF, DOCX, XLSX, PPTX, etc) permitidas para descarga en el INS, garantizando que se bloqueen archivos con extensiones de tipo ejecutables, librerías, imágenes ISO, en el firewall, con el fin de prevenir la descarga de malware en equipos del INS. Los referentes de proceso son responsables por mantener la lista blanca de extensiones actualizada, y realizar pruebas mensuales de la efectividad de la política configurada, garantizando así que solo se pueden descargar las extensiones permitidas.
PT016	Contratar un tercero especializado en el diseño e implementación de campañas de concienciación sobre el uso seguro adecuado de los sistemas de información y las plataformas tecnológicas del INS, con el objetivos de garantizar que personal de planta y contratistas aplican la seguridad de la información en el día a día. Los referentes de proceso deberán garantizar que el personal de planta y contratistas de su proceso asisten y/o participan de las campañas.
PT049	Evaluar el conocimiento entregado en las campañas de concienciación de seguridad de la información para identificar los aspectos a reforzar. Los referentes de proceso deberán recoger los resultados de las evaluaciones y realizar retroalimentación personalizada a las personas de sus correspondientes procesos.

PT037	Contratar un servicio de caza de amenazas de ciberseguridad (CTH) sobre la infraestructura tecnológica del INS, de manera que permita identificar vectores de ataque y debilidades a ser remediadas para evitar futuros incidentes de ciberseguridad.
PT020	Contratar un ejercicio de ingeniería social con enfoque en acceso físico, permitiendo identificar el nivel de vulnerabilidad con respecto a control de acceso a las instalaciones, verificación de información confidencial en canecas de basura (trashing), acceso a información mediante engaño a través de suplantación de identidad. Los referentes de proceso serán responsables por la implementación de los correspondientes planes de acción y recomendaciones resultado del ejercicio.
PT023	Implementar el etiquetado de los activos de información que fueron identificados, clasificados y valorados en el inventario de activos de información del INS de acuerdo al procedimiento definido. Los referentes de proceso deben garantizar que tanto el personal de planta como los contratistas del proceso cumplen con el procedimiento, realizando la retroalimentación necesaria en caso de encontrar incumplimientos.
PT025	Adquirir destructoras de papel en aquellas áreas que producen información documentada, con el fin de asegurar que la información clasificada como: Reservada y Clasificada, es desechada adecuadamente. Los referentes de proceso serán responsables por verificar el correcto funcionamiento de las destructoras, reportando oportunamente fallas o problemas en las mismas.
PT045	Ejecutar semestralmente simulacros de ocurrencia de incidentes de seguridad de la información para verificar que se actua de acuerdo a lo definido en el correspondiente procedimiento. Los referentes de proceso deberán garantizar la coordinación de los recursos requeridos para realizar el ejercicio.

PT040	Contratar un servicio de inteligencia de ciberamenazas de seguridad (CTI) para la infraestructura tecnológica del INS, de manera que permita reaccionar a tiempo ante ataques de ciberseguridad y a su vez proponer mejoras permanentes a la seguridad del INS.
PT024	Contratar una solución para el borrado seguro de la información electrónica, clasificada como: Reservada y Clasificada. La aplicación puede ser libre o comercial, sin embargo se debe garantizar que cumple estándares de borrado seguro como el DOD 5220.22. Los referentes de proceso deben realizar verificaciones trimestrales sobre la instalación y utilización de la herramienta de borrado seguro en los equipos/dispositivos donde aplique.
PT043	Cifrar los canales de comunicación a través de los cuales se intercambia información con entidades que se tengan convenios, de manera que se cumpla con las políticas definidas en el manual de políticas de seguridad de la información para el intercambio seguro de información.
PT041	Contratar el diseño de una red segura y su respectivo acompañamiento en la implementación de dicho diseño. Los referentes de proceso deberán participar en el diseño de la red segura suministrando información técnica actualizada de los sistemas de información o aplicaciones desarroladas o implementadas en el proceso.
PT042	Adquirir o renovar certificados digitales en las plataformas web criticas según resultados de análisis de vulnerabilidades e informe de ethical hacking. Los referentes de proceso deberán verificar semestralmente que las aplicaciones WEB de sus procesos tienen implementados los certificados digitales, es decir que se pueden acceder por HTTPS.

PLANES DE TRATAMIENTO

Tipo de plan de acción	Peso de evaluación del plan de acción	Efectividad del plan de acción	Plazo	Estado
Preventivo	100	Fuerte	Mediano plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	No planeado

Detectivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	Planeado
Preventivo	100	Fuerte	Corto plazo	No planeado

Detectivo	100	Fuerte	Mediano plazo	No planeado
Detectivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	No planeado
Detectivo	100	Fuerte	Mediano plazo	No planeado

Preventivo	100	Fuerte	Corto plazo	Planeado
Preventivo	100	Fuerte	Mediano plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Mediano plazo	No planeado
Detectivo	100	Fuerte	Mediano plazo	No planeado

Detectivo	100	Fuerte	Corto plazo	No planeado
Correctivo	100	Fuerte	Corto plazo	Planeado
Preventivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Mediano plazo	No planeado
Detectivo	100	Fuerte	Mediano plazo	No planeado

Detectivo	100	Fuerte	Mediano plazo	No planeado
Detectivo	100	Fuerte	Mediano plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	Planeado
Preventivo	100	Fuerte	Mediano plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	Planeado
Preventivo	100	Fuerte	Corto plazo	No planeado

Preventivo	100	Fuerte	Corto plazo	Planeado
Preventivo	100	Fuerte	Corto plazo	No planeado
Correctivo	100	Fuerte	Mediano plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	Planeado
Preventivo	100	Fuerte	Corto plazo	Planeado

Preventivo	100	Fuerte	Corto plazo	No planeado
Correctivo	100	Fuerte	Corto plazo	Planeado
Preventivo	100	Fuerte	Corto plazo	Planeado
Detectivo	100	Fuerte	Mediano plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	Planeado
Detectivo	100	Fuerte	Corto plazo	No planeado

Detectivo	100	Fuerte	Corto plazo	No planeado
Detectivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Mediano plazo	No planeado
Detectivo	100	Fuerte	Corto plazo	No planeado

Detectivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	No planeado
Preventivo	100	Fuerte	Mediano plazo	No planeado
Preventivo	100	Fuerte	Corto plazo	Planeado

Extremo	Alto	Moderado	Prioridad
252	221	91	1
187	314	86	2
178	0	23	3
131	18	89	4

131	18	89	5
120	0	16	6
115	9	59	7

105	228	16	8
98	95	40	9
87	51	18	10
63	60	13	11
63	44	17	12

56	111	0	13
49	51	5	14
48	270	66	15
48	12	18	16
47	55	24	17

46	34	0	18
45	53	18	19
45	19	38	20
44	142	8	21
43	12	1	22

37	20	6	23
31	104	18	24
29	19	10	25
28	0	0	26
24	1	12	27
20	9	14	28

17	0	4	29
16	1	0	30
15	55	2	31
15	50	5	32
15	50	5	33

15	50	5	34
12	1	0	35
12	0	12	36
12	0	0	37
11	2	8	38
9	45	0	39
9	45	0	40

8	9	1	41
7	6	1	42
7	6	1	43
7	6	1	44
7	6	0	45

6	16	1	46
6	0	2	47
6	0	0	48
3	1	2	49
0	34	2	50