1. **PROCESO:** Gestión de las tecnologías de la información

2. **SUB PROCESO:** NA.

3. **OBJETIVO:** Identificar, valorar, escalar, tratar y corregir vulnerabilidades asociadas a los incidentes de seguridad de la información.

4. **ALCANCE**: Inicia con el reporte de un evento y finaliza con el análisis de todos los incidentes reportados durante el semestre.

5. **DISPOSICIONES GENERALES:**

Es responsabilidad de todos los funcionarios y contratistas de la USPEC reportar cualquier tipo de incumplimiento a las políticas y procedimientos del SGSI, con el fin de detectar o detener incidentes de seguridad de manera oportuna y así buscar el tratamiento adecuado evitando que se afecten las propiedades de confidencialidad, disponibilidad e integridad de los activos de información.

Entre las anomalías más comunes que un usuario (Funcionario o Contratista) no administrador de tecnología puede llegar a evidenciar, se encuentran los temas relacionados en el **Anexo 1** - **Categorías Gestión de Incidentes – Generales** que pueden llegar a considerarse base de un supuesto incidente de seguridad.

En el caso de los administradores de tecnología o personal de monitoreo, se deben reportar anomalías en servidores, servicios o aplicaciones que se encuentren relacionados en el **Anexo 2** - **Categorías Gestión de Incidentes – Administración.**

Las actividades de contención de un incidente de seguridad pueden consistir en una o más de las siguientes tareas:

- Poner en cuarentena el o los equipos al interior de la red que estén causando el problema.
- Bloqueo del o los equipos por fuera de la red que estén causando el problema.
- Desconexión del servidor o servidores que estén siendo víctimas de un ataque informático.
- Bloqueo del tráfico por un puerto específico en cualquier sentido de transferencia.
- Cambio de prioridad en aplicaciones o en asignación de ancho de banda.
- Interrupción de actividades u operaciones afectadas por el incidente.

Para la remediación de vulnerabilidades pueden llevarse a cabo, entre otras, una o más de las siguientes tareas:

- Actualización de software.
- Desinstalación de software.
- Configuración de una nueva firma de ataque en el IDS e IPS.
- Configuración de un tipo de comportamiento anómalo en el IDS e IPS.
- Configuración de una VPN.
- Segmentación de tráfico con el uso de VLANs.
- Formateo o restauración del sistema de un equipo o máquina virtual.
- Endurecimiento del Sistema Operativo.
- Instalación de parches de seguridad liberados por los fabricantes.
- CAMBIO en la parametrización de aplicaciones.
- Habilitación de logs de auditoría.

- Establecimiento de nuevos procedimientos de monitoreo.
- Campañas de concienciación en Seguridad de la Información.

Trimestralmente, se debe realizar el análisis de todos los incidentes presentados validando si las acciones tomadas fueron efectivas, de lo contrario se debe realizar un Plan de Remediación diferente para cada Incidente que tenga reincidencia.

6. DEFINICIONES:

Activo: Cualquier elemento que tiene valor para la organización y que para Gestión de riesgos de seguridad de la información se consideran los siguientes: redes, hardware, información, ubicación, personal, procesos y actividades del negocio, software y estructura organizacional. [Fuente: ISO 27005].

Causas: La razón por la cual se sucede el evento y cuya identificación depende del nivel de experiencia sobre el entorno y los elementos involucrados.

Eventos: Presencia o cambio de un conjunto particular de circunstancias, que puede ser una o varias ocurrencias con una o varias causas. Un evento puede consistir en algo que no está sucediendo.
[Fuente: ISO 31000].

IDS: Sistema de detección de intrusiones. Es un programa de detección de accesos no autorizados a un computador o a una red.

IPS: Sistema de Prevención de Intrusiones. Es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Propietario del activo: Persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

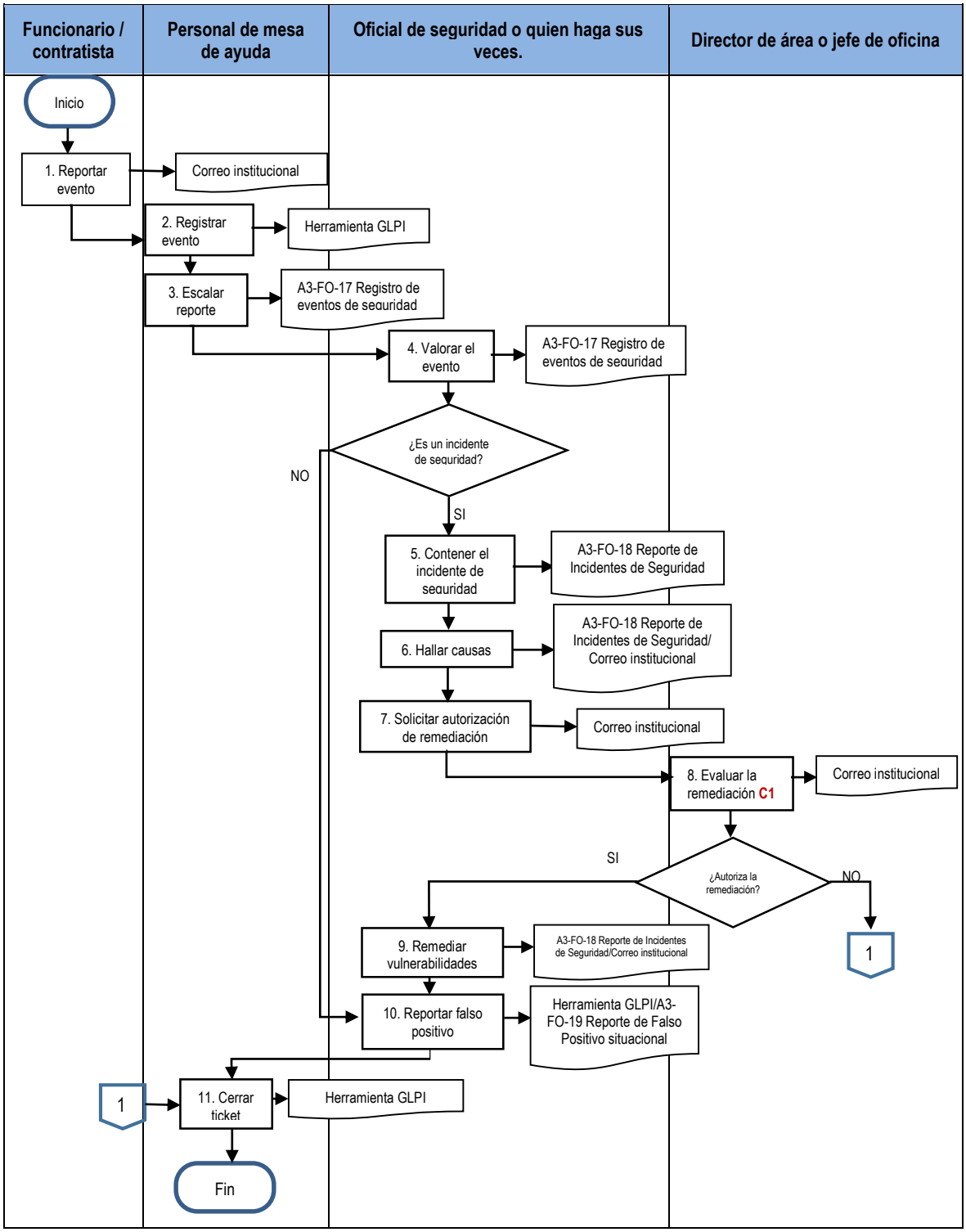
Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización) [Fuente: ISO 31000].

VLAN: Red de área local virtual, es un método para crear redes lógicas independientes dentro de una misma red física.

VPN: Red Privada Virtual, es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

Vulnerabilidad: debilidad identificada sobre un activo y que puede ser aprovechado por una amenazas para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

7. FLUJOGRAMA:



8. DESCRIPTIVO DEL PROCEDIMIENTO:

N°	Responsable	Registros	D Descripción de la actividad. Cx Punto de Control.	
1	Funcionario / Contratista	Correo institucional	**D**	**REPORTAR EVENTO:** El funcionario y/o contratista reporta cualquier evento que afecte el correcto funcionamiento de los sistemas y comunicaciones. Este reporte se deberá hacer a través de los canales de comunicación con la Mesa de Ayuda de acuerdo al procedimiento **A3-PR-01 Gestión de Solicitudes de Soporte Técnico.**
2	Personal de Mesa de Ayuda	Herramienta GLPI	**D**	**REGISTRAR EVENTO** El personal de mesa de ayuda registra el evento en la herramienta (GLPI).
3	Personal de Mesa de Ayuda	A3-FO-17 Registro de eventos de seguridad	**D**	**ESCALAR REPORTE** El personal de mesa de ayuda evalúa el evento y registra en el formato **A3-FO-17 Registro de eventos de seguridad**, diligenciando los campos correspondientes a la sección 1 “Descripción del Evento” y se envía por correo electrónico al Oficial de seguridad o quien haga sus veces.
4	Oficial de seguridad o quien haga sus veces	A3-FO-17 Registro de eventos de seguridad	**D**	**VALORAR EL EVENTO** Se realiza la valoración del evento de seguridad a través del formato **A3-FO-17 Registro de eventos de seguridad**, diligenciando los campos correspondientes a la sección 2 “Análisis del posible incidente” determinando si existe un incidente de seguridad. En dado caso que no sea tecnológico se especifica en el formato” Revisiones Adicionales” a que área corresponde. **¿Es un incidente de seguridad?** **Sí:** continúa con la actividad 5 **No:** Pasa a la actividad 10. El evento se tratará como un soporte técnico. (Ver **A3-PR-01 Gestión de Solicitudes de Soporte Técnico**).
5	Oficial de seguridad o quien haga sus veces	A3-FO-18 Reporte de Incidentes de Seguridad.	**D**	**CONTENER EL INCIDENTE DE SEGURIDAD** Tomando como base el reporte del incidente de seguridad se procede con la acción inmediata para contener el incidente y determinar el nivel de afectación sobre los activos. (Ver actividades de

				contención descritas en las disposiciones generales). Las acciones de contención se deberán registrar en el formato **A3-FO-18 Reporte de Incidentes de Seguridad** diligenciando los campos correspondientes a "Actividades de Contención".
6	Oficial de seguridad o quien haga sus veces	A3-FO-18 Reporte de Incidentes de Seguridad. Correo institucional	**D**	**HALLAR CAUSAS** Considerando toda la información recogida se procede con el análisis de las vulnerabilidades que deben ser corregidas para la erradicación del problema, una vez determinado esto se diligencian en el formato **A3-FO-18 Reporte de Incidentes de Seguridad** los campos correspondientes a "Análisis de Vulnerabilidades".
7	Oficial de seguridad o quien haga sus veces	Correo institucional		**SOLICITAR AUTORIZACIÓN DE REMEDIACIÓN** A través de correo institucional se le solicita al Dueño del proceso responsable del activo afectado, la autorización para corregir las vulnerabilidades detectadas, indicando los riesgos potenciales que se pueden generar si no se corrigen.
8	Director de área o Jefe de Oficina	Correo institucional	**D** **C1**	**EVALUAR LA REMEDIACIÓN** El dueño del activo de información sobre el cual se tiene el incidente, debe valorar la necesidad de corregir las vulnerabilidades contra el impacto en el funcionamiento de la USPEC y establecer si autoriza la corrección de las vulnerabilidades que permitieron el incidente, o procede a aceptar el riesgo que implica mantener la vulnerabilidad y notifica su concepto o justificación a través de correo institucional remitido al Oficial de Seguridad o quien haga sus veces. **¿Autoriza la remediación?** **Sí:** Continúa con la actividad 9 **No:** Pasa a la actividad 11
9	Oficial de seguridad o quien haga sus veces	A3-FO-18 Reporte de Incidentes de Seguridad.	**D**	**REMEDIAR VULNERABILIDADES** Con la autorización del dueño del activo de información, se debe proceder a remediar las vulnerabilidades que permitieron la causa del incidente de seguridad. (Ver posibles tareas de remediación en disposiciones generales). Se

		Correo institucional		notifica a Mesa de Ayuda la solución brindada al Incidente reportado.
10	Oficial de seguridad o quien haga sus veces	Herramienta GLPI A3-FO-19 Reporte de Falso Positivo	**D**	**REPORTAR FALSO POSITIVO** Se remite formato de Reporte de Falso Positivo diligenciado a la Mesa de Ayuda, con el fin de que se dé solución al evento como corresponde.
11	Mesa de Ayuda	Herramienta GLPI	**D**	**CERRAR TICKET** La mesa de ayuda realiza el cierre del ticket según la información brindada por el oficial de seguridad o quien haga sus veces, en la herramienta GLPI. Fin del procedimiento.

9. PUNTOS DE CONTROL:

Punto de Control	Responsable	Registro
C1 Autorizar la corrección de vulnerabilidades que permitieron la causa del incidente de seguridad de la información.	Director de área o Jefe de Oficina	Reporte de incidentes de seguridad autorizado.

RESUMEN DE CAMBIOS:

Versión	Fecha	Numerales	Descripción de la modificación
01		Todos	Se crea el documento

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma: Original Firmado	Firma: Original Firmado	Firma: Original Firmado
Nombre: Fernando Aguilera	Nombre: Elkin Prieto Santanilla	Nombre: Diana Pinilla
Cargo: Consultor Externo - Globaltek Security SAS	Cargo: Analista de Sistemas	Cargo: Jefe Oficina de Tecnología
Dependencia: NA.	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología

ANEXO 1

Categorías Gestión de Incidentes – Generales

C1_Control_ de Acceso

Bloqueo de cuenta debido a intentos de contraseña incorrecta
Acceso no autorizado
Denegación de privilegios

C2_Seguridad_de_Redes

Ataques externos a los activos
Ataques internos a los activos
Ataques contra la infraestructura IT

C3_Seguridad_Física

Problemas ambientales
Vandalismo o asonada
Acceso físico no autorizado
Pérdida o robo de computadores personales o portátiles
Pérdida o robo de dispositivos móviles (blackberry, PDA)
Pérdida o robo de infraestructura de red (routers, switches)
Pérdida o robo de otros activos tecnológicos (printers, token, RAM)
Pérdida o robo de dispositivos de almacenamiento (hard drives, backup tapes)
Daño o destrucción de equipos

C4_Antivirus

Malware (adware, spyware, activex, vbscript, backdoor, trapdoor)
Virus (gusanos, troyanos, hoax)
Suplantación (phishing, spoofing, vishing, smishing)
Ausencia de software antivirus
Software antivirus desactualizado o no configurado

C5_Manejo de la Información

Error en la entrega de datos (wrong recipient, email, fax, mail error)
Uso no autorizado de mensajería electrónica (carta cadena, spam)
Divulgación no autorizada de información confidencial
Pérdida de archivos
Divulgación no autorizada de datos
Pérdida de datos de clientes o datos personales
Integridad afectada

C6_Problemas de Disponibilidad

Mal funcionamiento o problemas de equipos
Error de configuración de aplicaciones

Daños de software

C7_Incumplimiento Normativo

Uso inapropiado de email
Préstamo de contraseñas
Uso de medios de almacenamiento no autorizados (USB, CD/DVD RW)
Vencimiento de licencias de software

C8_Otros

Reporte de debilidad de seguridad
Desastres naturales

ANEXO 2

Categorías Gestión de Incidentes – Administrador

C1_Control_ de Acceso

Bloqueo de cuenta debido a intentos de contraseña incorrecta
Acceso no autorizado
Sistema o aplicación que no cumple las políticas de contraseñas
Cuenta no autorizada o sin debida novedad
Privilegios de administración no autorizados
Denegación de privilegios
Modificación no autorizada de privilegios

C2_Seguridad_de_Redes

Eventos irregulares en la infraestructura de red
Eventos irregulares en dispositivos de seguridad perimetral
Conexión no autorizada de terceros
Pruebas de penetración no autorizadas
Cambios no autorizados en los dispositivos de seguridad perimetral
Uso no autorizado de utilitarios (rootkit)
Ataques contra servidores de nombre de dominios (DNS)
Ataques contra sistema cortafuegos (firewall)
Ataques externos a los activos
Ataques internos a los activos
Ataques contra sitios web
Ataques contra componentes de red (routers/switches)
Ataques contra sistemas de producción o contingencia
Ataques contra la infraestructura IT

C3_Seguridad_Física

Acceso físico no autorizado

Pérdida o robo de infraestructura de red (routers, switches)
Pérdida o robo de otros activos tecnológicos (printers, token, RAM)
Fallas en centros de datos o cuartos de comunicaciones
Consolas de administración sin protección

C4_Antivirus

Malware (adware, spyware, activex, vbscript, backdoor, trapdoor)
Virus (gusanos, troyanos, hoax)
Software antivirus desactualizado o no configurado

C5_Manejo de la Información

Uso no autorizado de mensajería electrónica (carta cadena, spam)
Divulgación no autorizada de información confidencial

C6_Problemas de Disponibilidad

Fallas en la recuperación de copias de seguridad (backups)
Fallas de generación de bitácoras (logs)
Mal funcionamiento o problemas de equipos
Denegación de servicio
Error de configuración de estaciones de trabajo
Error de configuración de aplicaciones
Daños de software
Producto próximo a quedar sin soporte (End Of Life)

C7_Incumplimiento Normativo

Uso inapropiado de email
Uso inapropiado de recursos tecnológicos
Uso inapropiado de internet
Préstamo de contraseñas
Cambios no autorizados en aplicaciones
Cambios no autorizados en configuraciones
Uso de medios de almacenamiento no autorizados (USB, CD/DVD RW)
Uso de software y/o hardware no autorizado
Vencimiento de licencias de software
Pruebas en ambientes de producción o contingencia

C8_Otros

Violación de controles de seguridad
Fraude o actividad criminal
Reporte de debilidad de seguridad