UNIVERSIDAD DE CALDAS

PLAN ESTRATÉGICO PARA AFRONTAR UN CYBERATAQUE

Agosto 2022

Tabla de contenido

INTRODUCCIÓN 3
ANTECEDENTES 3
VISIÓN 3
MISIÓN Y VALORES FUNDAMENTALES 4
PREVENCIÓN 4
- Política de seguridad 5
- Inventario de Servicios 5
- Monitoreo permanente de la infraestructura y sus servicios (FireWall) 5
- Monitoreo permanente de interacción de usuarios con la infraestructura y sus servicios ... 6
- Monitoreo del uso de la web 7
- Planes de capacitación en seguridad básica 7
- Protección del correo electrónico 8
- Incidentes de Seguridad 8
- Ataques de Red 9
- Plan de Recuperación ante desastres (RDP) 11
- Instalación de antivirus 11
- VPN y Segmentos de Red 12
- Sistema de Backups 12

Manejo del Ciberataque 12
IMPLEMENTACIÓN DE LA ESTRATEGIA ANTE UN CASO DE CIBERATAQUE 13
Trabajo preliminar 13
Elaboración plan estratégico – Borrador 14
Socialización plan estratégico – Equipo Directivo 14
Socialización plan estratégico – Comunidad Universitaria 14
Publicación y puesta en operación plan estratégico 14

INTRODUCCIÓN

Los ciberataques hoy por hoy son una real amenaza las 24 horas del día, los 7 días a la semana, los 365 días al año; los ciberdelincuentes no descansan. Con tan variada oferta y el rápido crecimiento de la infraestructura tecnológica en el mundo, son muchos los frentes que se deben estar monitoreando y vigilando: servidores Onpremises, servidores Cloud, redes WiFi, IoT, entre otros, hacen que la tarea sea un poco mas compleja cada día. Y es que las grandes empresas ya no son el único foco de interés para los delincuentes, todo aquello que represente centro de acopio de información será un blanco para sus propósitos, es aquí donde nuestros centros educativos aparecen en el radar.

Nota: Todas las imágenes y datos estadísticos son cifras reales, tomadas de los informes, entregados a la universidad por la empresa responsable de prestar el servicio de seguridad perimetral.

ANTECEDENTES

La realidad es que la dependencia del planeta a los servicios tecnológicos es cada vez mayor, en donde en el pasado, solo quienes tuvieran algún tipo de formación en tecnología accedían a este tipo de herramientas, hoy por hoy, mas del 90 % de las personas tiene acceso a servicios, algunos básicos como consultar redes sociales, juegos interactivos (jugadores de todo el mundo en línea), hacer una búsqueda en algún tipo de buscador, hasta algunos un poco mas especializados como hacer transacciones bancarias, encender o apagar la alarma de la casa de manera remota, entre otras. Y es aquí donde cualquier individuo que interactúe con tecnología (mucho o poco) se vuelve vulnerable solo con el hecho de estar conectado a internet. Si ir muy lejos, cualquier persona que este planificando su viaje de vacaciones, con la primera búsqueda de tarifas de hotel, en menos de un minuto tendrá su explorador inundado de ofertas asociadas a su viaje, y nos preguntamos: ¿cómo saben que mi siguiente paso era buscar el alquiler del auto?

VISIÓN

La Universidad de Caldas, en su plan de acción institucional 2019-2022, siguiendo su eje estratégico “UNIVESIDAD REGIONAL Y PUBLICA”, propósito # 3 “TRANSFORMACION DIGITAL” pretende posicionarse en el país como una Universidad

a la vanguardia en el uso de nuevas tecnologías, incorporándolas a su quehacer diario bajo todos sus ámbitos académicos, administrativos, socioculturales y de investigación, impulsando el emprendimiento y la innovación, teniendo como pilares una infraestructura moderna y robusta, y un equipo de trabajo con todas las competencias necesarias para garantizar en todo momento la seguridad informática.

MISIÓN Y VALORES FUNDAMENTALES

En aras de garantizar el funcionamiento continuo de la Universidad y todas sus actividades, y en la medida en que muchos de sus procesos estén asociados al uso de las tecnologías, se tendrán que diseñar estrategias que brinden la tranquilidad ante cualquier amenaza informática (ciberataque). Como primera medida a tener en cuenta es que la seguridad debe estar en cabeza de un equipo altamente capacitado, con amplia experiencia en el área de ciberseguridad, y que tengan a disposición herramientas automatizadas, que permitan una detección y contención temprana de cualquier tipo de amenaza, logrando cerrar esas brechas de seguridad de manera oportuna, no sin antes identificar el origen de la amenaza y su comportamiento.

Dentro de los principales objetivos del equipo de seguridad se encuentran algunos como:

- Detección temprana de incidentes
- Diagnóstico del incidente
- Gestión de incidente
- Reducir y minimizar los posibles daños
- Restaurar en el menor tiempo los servicios afectados
- Determinar causas y origen
- Implementar y documentar planes de mejora

PREVENCIÓN

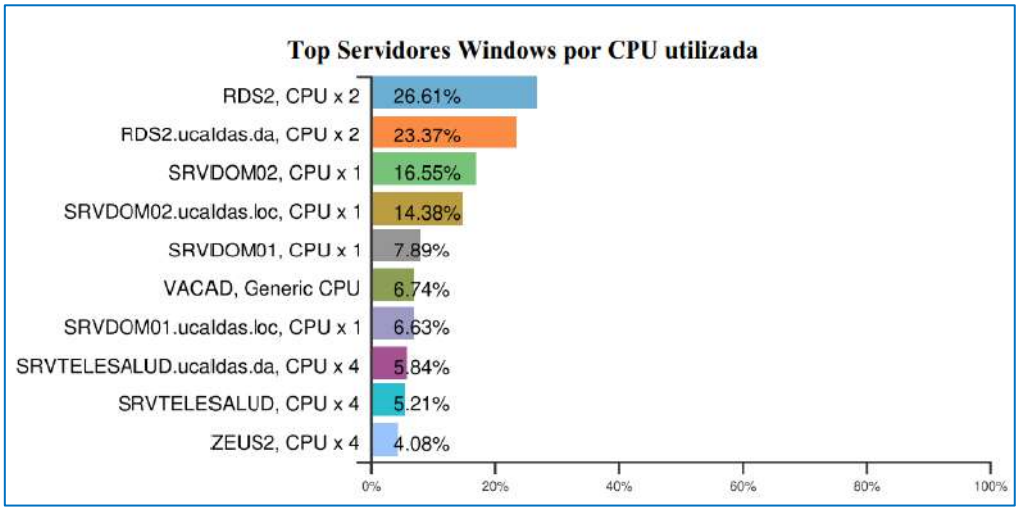
En cualquier caso, siempre va a ser más económico invertir en la prevención que en la recuperación. Existen algunos aspectos claves en el momento de prevenir cualquier tipo de amenaza o ciberataque, nombramos algunos como:

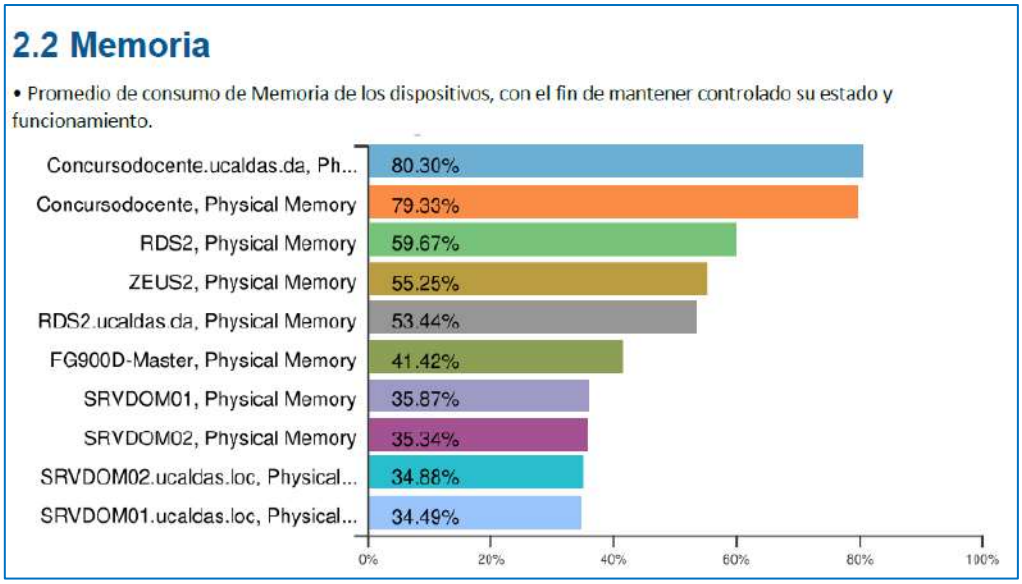
- **Política de seguridad**
  La Universidad debe contar con un manual de políticas de seguridad actualizado, pero lo mas importante es que sea permanentemente socializado con todos los actores de su ecosistema: "La cadena es tan fuerte como su eslabón más débil"

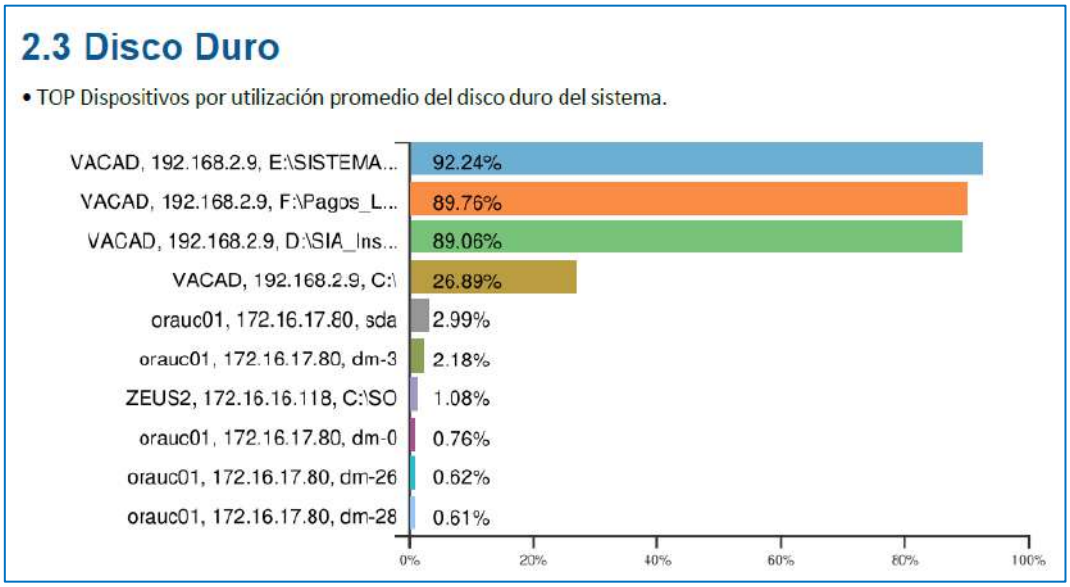
- **Inventario de Servicios**
  De manera preventiva, es importante que la universidad cuente con un inventario documentado y siempre actualizado de todos los servicios y su nivel de importancia en la operación, esto permitirá focalizar los esfuerzos de manera prioritaria en aquellos procesos que generen mayor impacto.

- **Monitoreo permanente de la infraestructura y sus servicios (FireWall)**
  Conocer la usabilidad normal de los servicios, nos permite identificar una línea base de consumo, de tal forma que ante cualquier variación atípica podamos actual de manera rápida antes de que se logre materializar la amenaza.

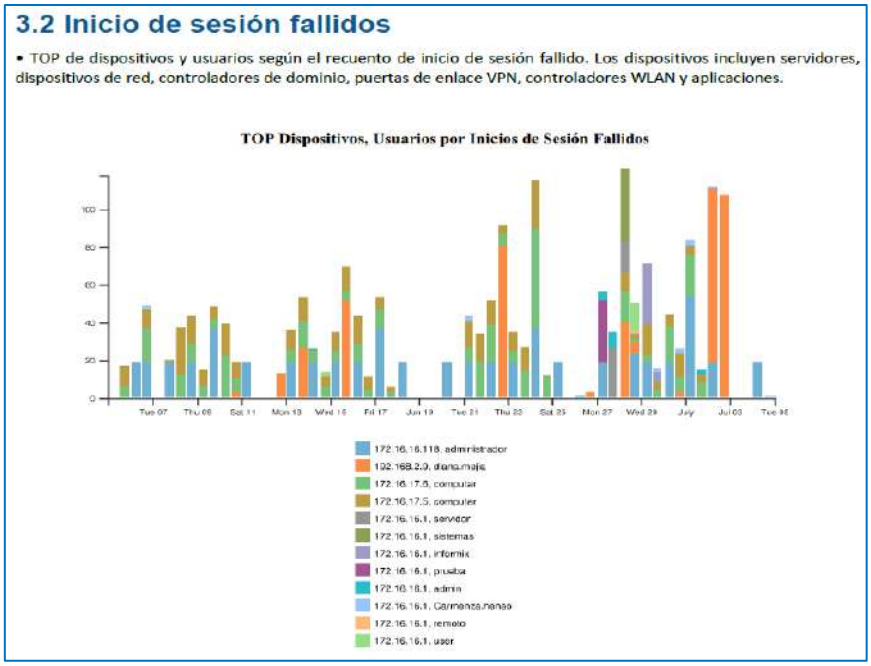
  En las siguientes gráficas encontramos el monitoreo detallado de algunos aspectos importante, como son: consumo de CPU, consumo de memoria, almacenamiento en discos duros:







- **<u>Monitoreo permanente de interacción de usuarios con la infraestructura y sus servicios</u>**
  Poder identificar el número de inicios de sesión fallidos y establecer algunas acciones de manera automática pueden llegar a ser acciones supremamente eficientes al momento de prevenir violación o accesos no permitidos.



- **<u>Monitoreo del uso de la web</u>**
  Según estudios en temas de ciber amenazas, los delincuentes prefieren tomar caminos cortos, y rara vez hacen lo contrario, por lo que medidas tan simples, como una autenticación con doble factor les exige un poco más de esfuerzo, logrando a veces su pérdida de interés frente al posible ataque.
  El monitoreo y restricción inteligente de los sitios que los usuarios frecuentan reduce notablemente los riesgos en la red.

- **<u>Planes de capacitación en seguridad básica</u>**
  Mantener bien informados a los usuarios de la red se convierte en una tarea primordial a la hora de brindar protección. En una red, cada uno de sus usuarios se convierte en una amenaza latente para todos, por ello la concientización de la responsabilidad compartida debe ser un tema de todos los días.

Los 20 usuarios más bloqueados

#	User (or IP)	Requests
1	10.15.1.9	457,707
2	10.15.1.15	69,630
3	10.14.1.4	24,228
4	10.15.9.48	9,430
5	10.23.0.86	6,230
6	10.17.0.58	5,808
7	10.2.101.12	5,648
8	10.17.0.37	5,288
9	10.11.60.36	4,552
10	172.16.20.32	4,443

Los 50 sitios más bloqueados

#	Website	Category	Requests
1	play[dot]google[dot]com	Freeware and Software Downloads	78,764,007
2	mask-h2[dot]icloud[dot]com	Proxy Avoidance	1,999,025
3	differentia[dot]ru	Malicious Websites	114,325
4	atomictrivia[dot]ru	Malicious Websites	106,218
5	login5[dot]spotify[dot]com	Internet Radio and TV	102,303
6	onlinecheck[dot]wildtangent[dot]com	Games	93,708
7	cuev[dot]in	Malicious Websites	93,567
8	mobilecrush[dot]king[dot]com	Games	64,074
9	vas[dot]samsungapps[dot]com	Freeware and Software Downloads	61,772
10	api[dot]itopvpn[dot]com	Proxy Avoidance	52,084
11	api[dot]peakgames[dot]net	Games	41,015

- **<u>Protección del correo electrónico</u>**
  Sin lugar a duda, una de las herramientas mas utilizadas en la actualidad es el correo electrónico, medio también utilizado para perpetrar ataques y lograr vulnerar la seguridad. Desde la validación misma del usuario en relación con los remitentes de confianza, hasta herramientas de escaneo para detección de amenazas son importantes para cerrar esta brecha.

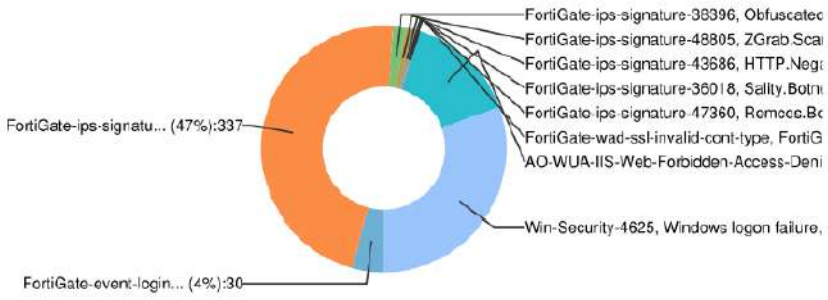
- **<u>Incidentes de Seguridad</u>**
  Contar con herramientas asociadas al firewall, nos permite identificar bajo el esquema de seguridad predictiva diferentes tipos de incidentes o eventos de seguridad en los equipos objeto de monitoreo, los cuales pueden llegar a tener una alta probabilidad de compromiso en la operación en caso de fallo. Los eventos deben ser clasificados

por su grado de severidad, a fin de concentrar la atención en aquellos que revisten mayor gravedad o amenaza.

4.2 Eventos de Seguridad

• Clasifica un TOP de eventos relacionados con la seguridad primero por su gravedad y luego por su recuento tod
los eventos mencionados a continuación fueron controlados sin afectar la infraestructura de la organización.

Top Eventos de seguridad



Rank	Event Name	Event Severity	COUNT(Matched Events)
1	Failed admin logon	10	30
2	Port.Scanning	7	337
3	Obfuscated.JavaScript.Access	7	12
4	ZGrab.Scanner	7	6
5	HTTP.Negative.Content.Length	7	3
6	Sality.Botnet	7	2
7	Remcos.Botnet	7	1
8	FortiGate wad ssl invalid cont type	7	1
9	Web request denied - forbidden access	5	106
10	Windows logon failure	3	218

- **<u>Ataques de Red</u>**

De manera continua, la infraestructura tecnológica es objeto de intervención maliciosa, cuyo objetivo es buscar vulnerabilidades en sus componentes y lograr penetrar sus sistemas. Dentro de los ataques mas comunes detectados por el sistema de seguridad perimetral de la universidad, encontramos los siguientes:

<u>SE-HSEO-01 - Evento de tipo Port.Scanning - Universidad de Caldas</u>

<u>Descripción</u>: Este evento indica la detección de un intento de escaneo desde un escáner de puertos; los escáneres de puertos, como Nmap, se utilizan para sondear redes informáticas para ver qué puertos o servicios están disponibles. La automatización de este tipo de herramientas nos permite tomar acciones de manera

inmediata, como es el bloqueo de direcciones MAC desde donde se venía generando el ataque, dando pie al inicio de una inspección por parte del equipo de soporte (validar el equipo involucrado, revisión de sus sistemas de antivirus, entre otros)

SE-HSEO-01 - Evento de tipo "DHCP Inanición" - Universidad de Caldas

Descripción: Este evento se genera cuando un atacante envía, de manera constante, múltiples solicitudes DHCP falsificadas utilizando diferentes direcciones MAC en el campo chaddr (componente de la dirección física de la tarjeta de red en el cliente), lo que puede ocasionar el agotamiento de los recursos de las direcciones IP de un servidor DHCP, causando que los clientes legítimos no puedan obtener direcciones IP, u ocasionando fallas en el correcto funcionamiento del servidor debido al agotamiento de los recursos del sistema

SE-HSEO-01 - Evento de tipo "HTTP.URI.SQL.Injection" - Universidad de Caldas

Descripción: Se trata de un intento de aprovechar una vulnerabilidad de inyección SQL. Como resultado, un atacante remoto puede enviar una consulta diseñada para ejecutar comandos SQL en un servidor vulnerable.

SE-HSEO-01 - Evento de tipo Andromeda.Botnet

Descripción: evento "Andromeda.Botnet" consiste en un malware que afecta a los ordenadores que presenten sistema operativo Windows que se encuentren sin protección antivirus en donde se descargan datos y configuraciones de sitios remotos y también permite la ejecución de archivos a distancia. Los ordenadores infectados con este malware pasan a ser parte de una botnet.
Las funcionalidades de la botnet Andromeda incluyen:

- Descarga y ejecución de software adicional.
- Robo de credenciales de acceso a algunos sitios web.
- Creación de proxy de salida en la máquina infectada

*Resumen ejecutivo de amenazas detectadas por nuestros sistemas de seguridad perimetral

- **<u>Plan de Recuperación ante desastres (RDP)</u>**
  Tener una hoja de ruta, con instrucciones claras y detalladas sobre cómo proceder ante incidentes no planificados como pueden ser un ciber ataque a gran escala, desastre natural, entre otros, es clave para lograr normalizar la situación. El tiempo de respuesta ante este tipo de incidentes es crucial, no solo para contener la situación, sino para iniciar con las labores de restablecimiento de los servicios, empezando por los mas críticos.
  Objetivos básicos:
  - Dar continuidad a los servicios académicos y administrativos de la institución
  - Definir roles y responsables ante los escenarios del incidente
  - Actuar de manera organizada ente los incidentes presentados
  - Garantizar la seguridad de la información y de sus componentes

- **<u>Instalación de antivirus</u>**
  Si bien, contar con un antivirus no nos da la garantía total de protección, si nos permite en gran medida minimizar las posibilidades de una infección, y por consiguiente poner en riesgo nuestra información local e institucional. Un correcto licenciamiento establece que de manera permanente y automática se están actualizando las bases de datos en cuanto a nuevos virus, malware, troyanos y demás amenazas.

- **VPN y Segmentos de Red**
  Por último, dentro de las prácticas mas recomendadas para garantizar accesos controlados a la red de manera remota, esta el uso de las VPN (*Virtual Private Network*), la cual permite cifrado de paquetes, y por consiguiente proteger tu información.
  En cuanto a la segmentación de red, es una práctica que además de favorecer el tráfico y desempeño de la red, también ayuda a bloquear una propagación de un ataque, reduciendo el alcance del mismo.

- **Sistema de Backups**
  Contar con un sistema de backups es una de las tareas principales en temas de prevención, sin embargo la recomendación va mas allá de tener copias de seguridad; es necesario estar monitoreando de manera periódica que nuestros Backups SI están siendo generados de manera correcta, para ello se sugiere realizar simulacros, los cuales nos van a permitir verificar que efectivamente la información esta siendo protegida y podrá ser restaurada ante un incidente real.

Manejo del Ciberataque

- ✓ Identificar servicios comprometidos
  Perfilar cada uno de los servicios comprometidos, así:
  Grado 1:
  Aplicación con tolerancia mínima que requiere recuperarse de forma inmediata (a 8 horas)
  Grado 2:
  Aplicación que debe levantarse en menos de 12 horas después de la declaración del desastre
  Grado 3:
  Aplicación que puede levantarse en menos de 24 horas
  Grado 4:
  Aplicación que puede levantarse después de 24 horas
- ✓ Bloquear la acción de la amenaza
- ✓ Implementar medidas de contención
- ✓ Activación de protocolos de seguridad ((RDP)
- ✓ Definir estrategia de recuperación de aplicaciones
- ✓ Definir estrategia de recuperación de comunicaciones
- ✓ Definir estrategia de recuperación de centro de cómputo
- ✓ Recuperación de los Servicios Críticos

- ✓ Despliegue del plan de comunicaciones

  Nota:

  Es necesario tener diferentes alternativas de comunicación con todos los usuarios (internos y externos), a fin de garantizar que la información pueda llegar a su destino de una manera oportuna. Y es que ante un ataque se pueden ver afectados nuestros sistemas de correo internos, sitios web, sistemas telefónicos, entre otros. Por otro lado, saber Informar a la comunidad la naturaleza e implicaciones de los incidentes es todo un arte, pues esta información debe ser precisa, pero no incendiaria; lograr que los usuarios tomen las medidas necesarias para contener una posible propagación de la amenaza es importante, al igual que ante las dificultades los usuarios puedan saber cómo proceder, cuanto tiempo esperar, que sistemas pueden o no consultar, qué medios no digitales pueden utilizar, etc.

  Tener presente que existen clientes, tanto internos como externos con alta prioridad, equipos directivos, proveedores, bancos, a los cuales la información debe llegar en el menor tiempo posible, debido a la importancia de los procesos en los cuales participan. Si el ataque está dirigido al sistema de tesorería, podemos concluir que el área financiera como los bancos tendrán que tomar medidas de contención en el menor tiempo posible.

- ✓ Reactivar servicios (de ser necesario en infraestructura alterna)
  En aras de dar continuidad a los servicios, de no ser posible el uso de medios tecnológicos, se tendrán que definir estrategias de otro tipo, a fin de lograr la operación.

  Una vez se tenga garantizado que el incidente fue resuelto, de manera controlada deberán ir entrando nuevamente en producción los servicios,

- ✓ Documentación actualizada y monitoreo de la infraestructura

IMPLEMENTACIÓN DE LA ESTRATEGIA ANTE UN CASO DE CIBERATAQUE

Trabajo preliminar
Definición del equipo humano responsable (Roles y responsabilidades)

- Asesor en Seguridad Informática
- Coordinador Grupo de Sistemas
- Equipo de Soporte – Sistemas

- Ingenieros de Apoyo Aplicativos
- Equipo de Seguridad Perimetral y Networking
- Coordinador Prensa y Comunicaciones
- Jefe Oficina Asesora de Planeación y Sistemas
- Líder Sistema Integrado de Gestión
- Líder Mesa de Ayuda
- Jefe Oficina Financiera
- Jefe Oficina de Tesorería
- Jefe Registro y Admisiones
- Jefe de Seguridad Física
- Otros

Acciones: Planificación y Socialización del alcance del proyecto, capacitación, mapa de riesgos, presupuesto y cronograma. Roles y actividades.
Tiempo: 3 meses (Agosto-Septiembre-Octubre de 2022)

Elaboración plan estratégico – Borrador
El equipo de trabajo diseñará un plan estratégico que permita afrontar y superar incidentes asociados al ataque cibernético.

Acciones: Diseño plan estratégico
Tiempo: 4 Meses (Noviembre – Diciembre – Enero - Febrero 2023)

Socialización plan estratégico – Equipo Directivo
Para su revisión y aprobación se presentará ante el equipo directivo de la Universidad el plan estratégico.

Acciones: Presentación plan estratégico
Tiempo: 1 Mes (Febrero de 2023)

Socialización plan estratégico – Comunidad Universitaria
Diseño y desarrollo de talleres de socialización del alcance y las responsabilidades de cada usuario ante el plan estratégico de atención de ciberataques.

Acciones: Socialización y capacitación
Tiempo: 3 Meses (Febrero – Marzo - Abril de 2023)

Publicación y puesta en operación plan estratégico
Acciones: Desarrollar Plan de comunicaciones
Tiempo: Abril de 2023