Plan de Respuesta a Incidentes – 2023 Ransomware

HuescaTelecom

Responsable: Fernando Gutiérrez, Responsable Ciberseguridad HuescaTelecom

Tabla de revisiones

Versión	Modificaciones	Fecha	Aprobado por
1.0	Primera versión del plan	26-04-2023	Director General HuescaTelecom

0. Índice

1. Introducción

El equipo de seguridad de HuescaTelecom, en colaboración con el equipo directivo, presenta el Plan de Respuesta a Incidentes de Rasnomware, con el objetivo de ayudar a la gestión de la organización antes, durante y después de ocurrir un incidente de seguridad.

En este documento se identificarán los roles y responsabilidades de cada persona implicada en la organización, así como los procedimientos que se llevarán a cabo para mejorar la seguridad de la organización ante cualquier incidente de seguridad.

Este documento deberá ser revisado y actualizado anualmente o cuando ocurra un incidente de seguridad. Deberá ser aprobado por el Director General de la organización.

1.1. Objetivo

El objetivo del Plan de Respuesta a Incidentes de Ransomware es que todos los miembros de la organización conozcan y apliquen un procedimiento rápido y eficaz para actuar ante un incidente de Ransomware. Este procedimiento incluirá medidas para comunicar de forma correcta los incidentes a quien corresponda tanto dentro como fuera de la organización. También incluirá los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

1.2. Alcance y usuarios

Este plan se aplica a todos los incidentes graves que amenazan con interrumpir cualquier actividad crítica dentro del alcance del Sistema de Gestión de la Seguridad de la Información (SGSI) por un periodo mayor al objetivo de tiempo de recuperación de cada actividad individual.

Los usuarios de este documento son todos los miembros de HuescaTelecom. Este documento está al alcance de todos los miembros de la organización y es confidencial, ningún miembro podrá distribuirlo a terceras personas sin previa autorización del equipo directivo.

2. Actuación frente al incidente

Para actuar de la mejor manera posible ante un incidente, se deben identificar las líneas de actuación que se realizarán por parte de la organización, con el objetivo de sufrir el menor daño posible y conseguir una rápida recuperación.

En cada línea de actuación se identificarán los equipos responsables, así como un líder o responsable de los mismos.

2.1. Preparación ante el incidente

En la actualidad, la mayor parte de las infecciones por ransomware están teniendo lugar por medio de engaños de ingeniería social, y aproximadamente casi el 75 % de las veces logran llevar a cabo el ciberataque.

Este proceso en responsabilidad de todos los miembros de la organización, aunque será liderado por los responsables de seguridad de HuescaTelecom.

CONCIENCIACIÓN Y FORMACIÓN

Por ello, es esencial formar y concienciar a nuestros empleados, enseñándoles a reconocer estas situaciones y cómo actuar en consecuencia. Para ello, los empleados deben conocer las políticas de seguridad de la información de HuescaTelecom, como las relativas a uso de redes WiFi, seguridad en el puesto de trabajo, etc.

Se realizarán charlas con el objetivo de informar a los trabajadores de la organización sobre como detectar, actuar y responder ante un incidente de ransomware. A su vez, se podrán realizar otras actividades como juegos de rol, simulaciones, etc.

IDENTIFICACIÓN DE ACTIVOS CRÍTICOS

A su vez, se deben identificar los activos críticos empresariales que podrían ser amenazados por una infección de ransomware, valorando su criticidad en un valor numérico del 1 al 10 en la siguiente tabla:

Activo	Nivel de Criticidad (1-10)
Servidor NAS	10
Servidor Web	8
Ordenadores y teléfonos de trabajadores	7
Infraestructura de red (Routers, Switches, etc.)	8
Sistema de alimentación Ininterrumpida (SAI)	8
Sistema de seguridad (CCTV, alarmas, etc.)	10
Conexión a Internet	10
Documentación almacenada en el NAS	10
Ordenadores y teléfonos de directivos	9
Software de gestión de la empresa	8
Copias de seguridad	10

SIMULACIONES

En el proceso de preparación ante incidentes, la organización HuescaTelecom realizará simulaciones de infecciones de ransomware, con el objetivo de conocer cómo actuar ante este tipo de incidentes para solucionarlo lo más rápido posible y buscar el menor impacto posible.

En la realización de estas simulaciones, se verán implicadas todas las personas e instituciones que estarían presentes en la respuesta a un incidente (empleados, empresas externas, autoridades, etc.).

COMUNICACIÓN DEL INCIDENTE

La comunicación del incidente a todas las partes implicadas es primordial en la gestión de incidentes. Para ello se creará un proceso de comunicación de incidentes, donde se detallará quién debe comunicar y quien debe ser comunicado.

PROCESO DE COMUNICACIÓN INTERNA

Dependiendo del rol empresarial y el departamento del trabajador que detecta algún comportamiento sospechoso que pueda dar lugar a un incidente, el proceso de comunicación será distinto.

1. El incidente es detectado por un trabajador de cualquier departamento.
2. El trabajador se pone en contacto inmediatamente con el director del departamento.
3. El director de departamento contacta inmediatamente con el responsable de ciberseguridad de la organización.
4. El responsable de ciberseguridad, contacta con el Director General de la organización.
5. El Director General se comunica con todos los directores de departamento, comunicando el incidente a los mismos.
6. A su vez, el director general contacta con el responsable de ciberseguridad y el responsable de seguridad de la organización, para informar de que se va a aplicar el plan de respuesta a incidentes.
7. Finalmente, cada director de departamento comunicará a los empleados pertenecientes a su departamento mediante reunión, llamada telefónica o correo electrónico el contexto de la amenaza y cómo deben actuar.

Para un proceso de comunicación ágil y eficiente, al final del presente documento se muestra el Anexo I – Datos de contacto, donde se especifican todas las formas de contacto de todos los miembros de la organización.

A su vez, los directores de departamento recibirán una copia en papel del Plan de Respuesta a Incidentes en caso de sufrir el incidente, así como los anexos necesarios. Este documento deberá ser almacenado en formato papel, nunca en formato digital

PROCESO DE COMUNICACIÓN EXTERNA

El proceso de comunicación del incidente a las partes externas, tendrá como responsable al director del departamento de RR.HH. El objetivo de este proceso es comunicar a las personas y entidades ajenas a la organización sobre el incidente ocurrido. Para ello, se deberá tener en cuenta a quién se debe informar y cómo se debe informar.

Es por eso, que el director de RR.HH, en colaboración con otros empleados de la organización, comunicarán sobre el incidente de la siguiente manera:

- ✓ Creación de un comunicado oficial que deberá ser redactado y aprobado en conjunto por todos los directivos de la organización. Este comunicado será compartido en la página web de la organización y en las redes sociales.
- ✓ Los responsables de seguridad se pondrán en contacto con las autoridades pertinentes con el objetivo de trabajar conjuntamente para hacer frente al incidente.
- ✓ Los responsables de seguridad, en caso de ser necesario, se pondrán en contacto con una empresa externa de asesoramiento, con el objetivo de recibir ayuda para la respuesta al incidente.
- ✓ En caso de recibir alguna solicitud de entrevista por parte de algún medio de comunicación, será el director de RR. HH quién responda a las preguntas.
- ✓ Se enviará un mensaje (correo electrónico, SMS, etc.) a los clientes afiliados con la empresa, informando sobre el incidente.
- ✓ Se contactará con los clientes en caso de ser necesario.

CHECKLIST PREPARACIÓN DEL INCIDENTE

Para una correcta preparación ante un incidente, se deben cumplir una serie de controles para revisar el cumplimiento de la política de seguridad de la organización.

Los controles se clasificarán en dos niveles de complejidad:

- ➢ Básico (B): el esfuerzo y los recursos necesarios para implantarlo son asumibles.
- ➢ Avanzado (A): el esfuerzo y los recursos necesarios para implantarlo son considerables.

Los controles podrán tener el siguiente alcance:

- Procesos (PRO): aplica a la gestión del incidente.
- Tecnología (TEC): aplica al personal técnico de la gestión del incidente.
- Personas (PER): aplica a todo el personal.

Veáse el Anexo II – Checklist para la preparación del incidente, donde se especifican la serie de controles a llevar a cabo en la preparación para la gestión de un incidente.

RESPONSABILIDADES EN LA RESPUESTA A INCIDENTES

Las responsabilidades en la respuesta a incidentes se muestran en la siguiente tabla:

Rol empresarial	Responsabilidades/autorizaciones
Director General	Responsabilidad máxima en todos los ámbitos de la organización.
Responsable Ciberseguridad	Responsable de la gestión del incidente en la parte técnica. Responsable de la formación del equipo técnico de respuesta a incidentes
Director dep. RR.HH	Responsable de la gestión de la comunicación del incidente (interna y externa)
Director dep. Operaciones	Responsable de la continuación del trabajo durante el incidente (organización)
Director dep. Informática	Liderará, junto al responsable de ciberseguridad, el equipo técnico de gestión de incidentes

2.2. Contención de la amenaza

El objetivo de la fase de contención de la amenaza es evitar que:

- ✓ El código dañino no continúa propagándose por la red (cifrado de carpetas compartidas, movimiento lateral a otros equipos de la red, etc.).

- ✓ Si el atacante tiene conexión remota, deberá ser interrumpida de inmediato para evitar que pueda continuar con su actividad (exfiltración de datos, puertas traseras, cifrado de archivos, destrucción de evidencias, etc.).

En la gran mayoría de infecciones de Ransomware, el usuario se da cuenta de que ha sido infectado cuando el programa ha finalizado su ejecución y se muestra el mensaje de que todos los ficheros han sido encriptados, solicitando un rescate. Sin embargo, existe la posibilidad de que no haya finalizado su ejecución, pudiendo evitar el cifrado completo de los ficheros.

Debido a ello, en un incidente de ciberseguridad, en especial en el caso de un Ransomware, se debe proceder de forma inmediata a realizar las siguientes acciones:

2.2.1. Desconexión de los equipos de la red

Al producirse una infección por Ransomware, se comienzan a cifrar los ficheros del equipo y las unidades conectadas, tanto dispositivos físicos (discos duros externos, USB's, tarjetas SD, etc.) como dispositivos de red.

Los pasos a realizar en el momento de detectar un Ransomware son:

1. Desconectar las unidades de red: Para ello, desconectar el cable de red del equipo, o en caso de funcionar por WiFi, desactivar las interfaces de red. Mediante esta acción podemos evitar el cifrado de ficheros en unidades de red accesibles, siempre y cuando el Ransomware no haya finalizado su ejecución.
2. Comprobar si el proceso dañino sigue ejecutándose: Esta tarea puede llegar a ser muy complicada, ya que el proceso dañino puede haber sido inyectado en un proceso legítimo, o simplemente podría haber finalizado su ejecución, lo que haría imposible comprobarlo.

   En caso de haber localizado el proceso dañino (mediante el administrador de tareas, por ejemplo), se realizará un volcado de memoria del proceso en concreto, pudiendo de esta manera estudiarlo con herramientas como *Volatility*. Este volcado deberá ser guardado en un sistema aislado.

3. Finalizar la ejecución del proceso dañino: Existe dos alternativas para finalizar el proceso dañino:
   - ✓ Acceder al Administrador de Tareas de Windows, click derecho sobre el proceso y elegir la opción 'Finalizar el árbol de procesos'.

- ✓ Si no se ha localizado el proceso dañino, apagar el equipo de manera manual e inmediata.

4. Arrancar el equipo en modo seguro: Antes de arrancar Windows de manera convencional, se pulsará la tecla F8 para acceder al menú de arranque avanzado, desde el que se seleccionará el arranque en "Modo Seguro". De esta forma, evitaremos que el Ransomware vuelva a activarse en caso de ser persistente y que no se hubiera eliminado con los procedimientos anteriores.
5. Realizar una copia de seguridad del equipo: Esta copia contendrá tanto los ficheros cifrados como no cifrados. Deberá realizarse en un dispositivo de almacenamiento aislado y fuera de la red. Aunque no se puedan descifrar los ficheros cifrados, no se deben eliminar, ya que es posible que en el futuro se rompa el cifrado o se descubran las claves de *Command and Control*.

2.2.2. Segmentación de la red

Esta probablemente sea la parte más importante en la gestión de un incidente de Ransomware.

Normalmente, el Ransomware es capaz de propagarse por la red a través de unidades compartidas en el dominio de la organización. Sin embargo, las tendencias en las últimas campañas en las que se encuentra involucrado el Ransomware también puede existir código dañino adicional para añadir mayor capacidad y complejidad. En algunos casos, se ha observado que se pueden producir escalados de privilegios, movimiento lateral por la red utilizando credenciales comprometidas, arrancar equipos apagados de la red y exfiltrar información.

El equipo técnico de respuesta a incidentes tendrá que rediseñar la red y establecer el punto idóneo para ubicar el firewall. El firewall permitirá tener visibilidad de todo el tráfico de la red que pase por él, esto será muy útil al disponer de IOC (indicadores de compromiso) para localizar equipos de la red que quieran establecer comunicaciones con servidores de mando y control.

En el Anexo IV – Posible diseño de la red para la contención de un Ransomware, se muestra una posible configuración de red que se debería diseñar para la contención de un Ransomware.

2.2.3. Despliegue MicroClaudia

Para finalizar la fase de contención, se desplegará una solución EDR (Endpoint Detection and response) en los puntos finales, equipos cliente y servidores, mejorando así la capacidad de detección y aislamiento.

MicroClaudia es una herramienta del CCN-CERT que distribuye vacunas específicas para cada caso de ransomware. Esta herramienta genera actuaciones que permite el bloqueo inmediato de cualquier malware relacionado con Emotet,Trickbot, Bitpaymer, Ryuk y Sodinokibi entre otros, de forma que se pueda detener la ejecución de los mismos en caso de que los equipos estén infectados o el código dañino intente propagarse.

2.3. Detección de la amenaza

En esta fase se procede a detectar que equipos han sido infectados por el código dañino, bien porque el atacante los hubiera utilizado para pivotar por la red o para cifrar y/o eliminar su contenido.

Durante esta fase se desarrollarán las siguientes acciones:

2.3.1. Instalación de la sonda SAT

El CCN-CERT dispone de una sonda, Sistema de Alerta Temprana que realiza las funciones de IDS y que puede ser desplegada en un punto de la red donde se tenga visibilidad de todo el tráfico entrante y saliente.

Permite identificar si, en base a los patrones conocidos por el CCN-CERT, existe tráfico categorizado como dañino en la red, de forma que se pueda actuar de manera oportuna para localizar y neutralizar la amenaza.

Para más información sobre el despliegue, véase Anexo V – Despliegue sonda SAT.

2.3.2. Instalación MicroClaudia

MicroClaudia es una herramienta del CCN-CERT que distribuye vacunas específicas de cada ransomware y así evita la ejecución de los mismos. Se instala en los equipos finales y contiene detectores de actuación basados en la investigación de los diferentes tipos de ransomware.

2.3.3. Investigación del código dañino

Una vez localizados los equipos afectados, en caso de haber localizado el código dañino y extraído el mismo a un lugar seguro, se procederá a investigar el mismo mediante herramientas de análisis de código dañino.

El objetivo es recopilar toda la información posible de la amenaza, incluyendo características, funcionalidad, conectividad, persistencia, indicadores que permitan su detección, etc.

Para obtener mayor información sobre las herramientas de análisis de malware, véase Anexo X – Herramientas de investigación de código dañino.

2.4. Mitigación de la amenaza

De forma simultánea a la contención y detección de la amenaza, se puede llevar a cabo la fase de mitigación, que consiste en neutralizar de forma efectiva el malware que ha infectado los equipos. Para ello se pueden seguir una serie de procedimientos, que se exponen a continuación.

2.4.1. Rediseño de la red

Una vez el atacante obtiene credenciales de dominio, comprometiendo previamente un equipo de la red, podría empezar a moverse lateralmente, buscando los equipos críticos con el objetivo de robar, cifrar o eliminar datos.

Teniendo en cuenta la naturaleza de los equipos y servidores, una red correctamente segmentada mediante la utilización de firewalls y separando los distintos entornos, el impacto potencial de un ransomware sería menor que una red que no está segmentada correctamente. A su vez, la segmentación permitiría aislar los equipos afectados durante un incidente de seguridad, impidiendo que el código dañino pudiera propagarse por la red para conseguir comprometer el Controlador de Dominio, lo que infectaría toda la red.

2.4.2. Actualización de los equipos

Es imprescindible que periódicamente se continué dando soporte y mantenimiento en forma de parches y actualizaciones a los equipos de la organización. Esto reducirá el número de vías de ataque potenciales, ya que el las actualizaciones se suelen implantar parches para reducir las vulnerabilidades de los equipos.

2.4.3. Cambio de credenciales en el dominio

Cuando una red ha sido vulnerada, ya sea mediante la explotación de una vulnerabilidad en alguno de los servicios expuestos a Internet o mediante ataques de phishing a través del correo electrónico de alguno de los miembros de la organización, el atacante tratará de escalar privilegios en la máquina comprometida con el objetivo de hacerse con las credenciales del equipo y del dominio.

Por ello, se resetearán las credenciales del dominio, una vez reconstruido el Controlador de Dominio y el Directorio Activo.

2.4.4. Comprobación del listado de usuarios en el dominio

Cuando un atacante consigue acceso a un equipo de la red, es común que cree algún usuario con el objetivo de seguir metido en la red de la organización mediante la creación de una puerta trasera.

Con el objetivo de evitarlo, se revisará el listado de todos los usuarios pertenecientes al dominio después de haber sido infectados y se comparará con el listado de usuarios antes de haber sufrido el incidente, prestando atención en las cuentas con privilegios de administrador o en las cuentas con un privilegio elevado.

Véase Anexo XI – Listado de usuarios pertenecientes al dominio para obtener el listado de usuarios de la organización anterior al incidente.

2.5. Recuperación de la información y servicios

Esta parte se puede realizar en a la vez que el resto. En un incidente de ransomware donde se han cifrado y borrado activos, es fundamental establecer el alcance del incidente, evaluando que información hay que recuperar y que servicios se han visto afectados.

2.5.1. Contextualización del escenario

En primer lugar, se necesita realizar una valoración del impacto producido por el ransomware, con el objetivo de intentar recuperar los ficheros cifrados. A continuación, se muestran alguno de los posibles escenarios, partiendo del más favorable al más desfavorable.

Cabe recordar que el pago del rescate solicitado no es una opción, ya que no garantiza que los atacantes envíen la clave de descifrado, además que les motiva a seguir distribuyendo de forma masiva este tipo de códigos dañinos.

ESCENARIO 1 – SE DISPONDE DE COPIAS DE SEGURIDAD COMPLETAS DEL EQUIPO

En caso de disponer backups completos de los equipos, en primer lugar, se procedería a la desinfección del equipo para posteriormente restaurar la copia de seguridad.

ESCENARIO 2 – EXISTE UNA HERRAMIENTA DE DESCIFRADO

En ocasiones existen herramientas públicas para restaurar los archivos cifrados por diferentes tipos de ransomware específicos, aunque desafortunadamente, sólo unas pocas variantes de ransomware son descifrables, ya sea porque se han obtenido las claves de cifrado tras intervenir el servidor de comando y control o porque existe una vulnerabilidad conocida en el código dañino que permite el descifrado de los archivos.

ESCENARIO 3 – SE DISPONE DE SHADOW VOLUME COPY

Shadow Volume Copy permite realizar backups automáticos o manuales de ficheros o volúmenes. A su vez, permite analizar un estado anterior del equipo para determinar un suceso, mediante el uso de instantáneas.

En caso de disponer de estos backups, bastaría con restaurar estas copias de seguridad automáticas mediante alguna herramienta como Shadow Explorer, aunque en muchos casos el ransomware imposibilita esta acción.

ESCENARIO 4 – SE PUEDEN RECUPERAR LOS FICHEROS CON SOFTWARE FORENSE

En algunas ocasiones es posible recuperar archivos eliminados por el ransomware mediante herramientas forenses.

Algunas de estas herramientas son:

- ✓ EaseUS Data Recovery Wizard
- ✓ Foremost
- ✓ Photorec
- ✓ Gparted
- ✓ Magnet Forensics
- ✓ Wondershare Recoverit
- ✓ Exterro (AccessData)
- ✓ X-Ways Forensics
- ✓ BlackBag Technologies

- ✓ Cellebrite
- ✓ CERT Triage Tools

Cuantas más herramientas de recuperación de archivos se utilicen, aumenta la probabilidad de recuperar un número de archivos eliminados mayor, ya que no todas las herramientas son capaces de recuperar el mismo número de archivos.

ESCENARIO 5 – NO HA SIDO POSIBLE DESCIFRAR Y/O RECUPERAR LOS DATOS

En caso de no haber podido descifrar los archivos afectados, se deben conservar los ficheros cifrados en un equipo aislado, ya que es posible que en el futuro puedan ser descifrados con una herramienta específica.

2.5.2. Inventariado de equipos afectados

Identificar el número de equipos afectados es necesario para determinar el alcance de la infección y el impacto del incidente. Con el objetivo de un inventariado rápido y eficaz, se rellenará una lista con los servicios afectados teniendo en cuenta la información que fue cifrada o eliminada.

Para obtener la lista a rellenar, véase Anexo XII – Listado de equipos afectados. Esta lista contendrá cuatro campos a rellenar, los cuales son:

- ✓ Equipo: descripción del equipo (Ej: Windows 10 empleado Dep. Operaciones, Servidor NAS, etc.)
- ✓ Datos: aquí se especificará los datos que contiene el equipo.
- ✓ Impacto: se establecerá el impacto que tiene el incidente en ese equipo y lo que supone para la organización.
- ✓ Estado: estado actual del equipo (Ej: recuperación completa, recuperación parcial, cifrado, etc.).

2.5.3. Recuperación de servicios afectados

Para la recuperación de los servicios afectados, se recomienda:

- ✓ Servicio Shadow Copy Volume.
- ✓ Recuperar las copias de seguridad.
- ✓ Utilizar herramientas de descifrado.
- ✓ Implantación microClaudia

2.6. Prevención

Se deberán establecer las políticas y mecanismos de seguridad necesarios para asegurar la prevención de una nueva infección que siga sin patrones similares a los expuestos anteriormente. Para ello, se procederá a actualizar las políticas y métodos de seguridad de la organización, además de mejorar el sistema de gestión de copias de seguridad.

2.6.1. Actualización de políticas de seguridad

Una vez aplicadas las tareas de desinfección y mitigación del código dañino en los equipos, será necesario:

- ✓ Deshabilitar la ejecución de scripts.
- ✓ Deshabilitar la ejecución de macros.
- ✓ Obligar a utilizar contraseñas robustas, mediante la implantación de gestores de contraseñas
- ✓ Utilizar 2FA para el acceso a cuentas empresariales
- ✓ Revisar el listado de usuarios pertenecientes al dominio, especialmente los que tienen altos privilegios o privilegios de administrador.
- ✓ Concienciación y formación de los miembros de la organización.
- ✓ Implementación de firewalls, IDs, Ips, SIEM, etc.

2.6.2. Actualizaciones de los métodos de seguridad en la red

En términos de red, es necesario establecer las políticas adecuadas para permitir el control de las conexiones que se puedan establecer en nuestra red. Para ello se aconseja seguir las siguientes recomendaciones:

- ✓ Bloquear mediante firewall conexiones no necesarias. Uso de listas blancas.
- ✓ Registrar toda la actividad de los equipos de la red.
- ✓ Implantación de SIEM, IPS, etc.
- ✓ Monitorización de la red.
- ✓ Reglas de detección anti-spam

2.6.3. Sistemas de copia de seguridad

Utilizar copias de seguridad es probablemente la mejor medida para gestionar un incidente de ransomware, ya que nos permiten recuperar todos los archivos cifrados y/o eliminados (en caso de que las copias de seguridad no hayan sido cifradas).

Para una correcta gestión de las copias de seguridad, es recomendable seguir las siguientes recomendaciones:

- ✓ Crear copias diarias, al menos, de los equipos críticos de la organización.
- ✓ Aislamiento de los servidores de copias de seguridad respecto al resto de la red, de manera que al ser nuestra red infectada el malware no pueda llegar directamente a nuestro servidor.
- ✓ Asegurarse de disponer de almacenamiento suficiente para mantener más de una copia de seguridad del mismo activo, ya que en caso de ser infectados y que el malware llegue a los backups, se pueda disponer de una copia anterior que no esté cifrada.
- ✓ Mantener copias de la información crítica de la organización en formato papel (si es posible) con el objetivo de garantizar que esa información no pueda ser corrompida o eliminada por ningún tipo de malware.
- ✓ Realizar periódicamente copias de seguridad que se encuentren físicamente aisladas y desconectadas de la red (al menos anualmente).

3. Mejora continua

El Plan de Respuesta a Incidentes se irá actualizando continuamente tras la realización de simulaciones y mediante la aplicación del mismo cuando se sufre un incidente. El objetivo es añadir procedimientos cada vez que se actualiza el plan. De esta forma se conseguirá una mejora continua del mismo, lo que ayudará a una mejor respuesta al incidente.

Para conseguir una mejora del plan, se debe:

- ✓ Realizar investigaciones.
- ✓ Crear un proceso de colaboración y comunicación entre las partes implicadas.
- ✓ Presentar informes con los resultados obtenidos tras aplicar el plan de respuesta a incidentes.
- ✓ Realización de reuniones donde los trabajadores expondrán sus ideas, quejas, etc.
- ✓ Generar estadísticas de cómo se ha aplicado el plan de respuesta a incidentes (tiempo utilizado, número de servicios afectados, número de servicios recuperados, número de servicios no recuperados, etc.). El objetivo de estas estadísticas es comparar cuál ha sido el resultado al aplicar el plan de respuesta, comparándolo con versiones anteriores, lo que nos ayudaría a sacar conclusiones sobre el plan de respuesta a incidentes.

El objetivo es recopilar toda esta información y adoptar medidas para adoptar mejoras en nuestros sistemas.

4. Referencias y enlaces de interés

microClaudia: https://www.ccn-cert.cni.es/soluciones-seguridad/microclaudia.html

SAT: https://www.ccn-cert.cni.es/gestion-de-incidentes/sistema-de-alerta-temprana-sat.html

5. Anexos

Anexo I – Documentación de interés

Análisis de activos y riesgo empresarial HuescaTelecom - 2023:
https://docs.google.com/spreadsheets/d/1rTQhdNv3sx8eRLwe46Kkz-E-3GxR3wsusPezbYHmk74/edit?usp=share_link
Marco Normativo HuescaTelecom – 2023:
https://docs.google.com/document/d/1GE4BrZm39-_Rax-_XpAIt_9A7pkM1-M_XHETDCSh7Zk/edit?usp=share_link
Normativa Global de Seguridad HuescaTelecom – 2023:
https://docs.google.com/document/d/131FY8emBa3vkPYBF0Xra9nudLWwlLSkImjL64XG55hY/edit?usp=share_link
Organización de Seguridad HuescaTelecom – 2023:
https://docs.google.com/spreadsheets/d/1tdDNP8z-4_tBRnfO-MUB8nN4529Q6EbFx2S6Rm-16gU/edit?usp=share_link
Política Global de Seguridad HuescaTelecom – 2023:
https://docs.google.com/document/d/1drU9j0SBh8V19MoflmnpJAjqsvAQCJ06SvFxepK6EaI/edit?usp=share_link

Anexo II - Datos de contacto

EQUIPO DIRECTIVO			
Rol	Teléfono	Correo electrónico	N.º Ext
Director general	*619876590*	*evillacampa@huescatelecom.com*	*910*
Director Comercio	654329876	jjfernandez@comerciohtelecom.com	210
Director RR.HH	632876900	clopez@recursoshtelecom.com	110
Director Operaciones	623140823	fcastiella@operacioneshtelecom.com	410
Director Finanzas	648733909	dramirez@finanzashtelecom.com	510
Director Informática	600754329	gcarvajal@informahtelecom.com	610
Responsable ciberseguridad	678549005	fgutierrez@cibersechtelecom.com	310
Responsable seguridad	629090861	rsanchez@sechtelecom.com	710

DEPARTAMENTO DE FINANZAS			
Nombre	Teléfono	Correo electrónico	N.º Ext
Daniel Ramírez	*648733909*	*dramirez@finanzashtelecom.com*	*510*
Héctor Jaén	698345007	hjaen@finanzashtelecom.com	511
Cecilia Calderón	690886621	ccalderon@finanzashtelecom.com	513
Angelita Balaguer	635789011	abalaguer@finanzashtelecom.com	514
María Sandoval	698022546	msandoval@finanzashtelecom.com	515
Francisco Martinez	630874568	fmartinez@finanzashtelecom.com	516
Isabel Benitez	684705641	ibenitez@finanzashtelecom.com	517
Dolores Valverde	679541054	dvalverde@finanzashtelecom.com	518

DEPARTAMENTO DE OPERACIONES			
Nombre	Teléfono	Correo electrónico	N.º Ext
Fernando Castiella	*623140823*	*fcastiella@operacioneshtelecom.com*	*410*
Javier Casal	678332768	jcasal@operacioneshtelecom.com	411
Fidel Llopis	684739522	fllopis@operacioneshtelecom.com	412
Rebeca Sevilla	685249344	rsevilla@operacioneshtelecom.com	413
Agustín Cantero	600238495	acantero@operacioneshtelecom.com	414
Antonio Lucena	622684756	alucena@operacioneshtelecom.com	415
Martina Mateu	699835762	mmateu@operacioneshtelecom.com	416
Fabián Carranza	641285398	fcarranza@operacioneshtelecom.com	417
Juan Calvo	653789854	jcalvo@operacioneshtelecom.com	418
Salvador Ortiz	619828232	sortiz@operacioneshtelecom.com	419
Manuela Requena	680980650	mrequena@operacioneshtelecom.com	420

DEPARTAMENTO DE RECURSOS HUMANOS			
Nombre	Teléfono	Correo electrónico	N.º Ext
Carlos López	*632876900*	*clopez@recursoshtelecom.com*	*110*
Blanca Vicens	622147630	bvicens@recursoshtelecom.com	111
Carlota Prieto	639001298	cprieto@recursoshtelecom.com	112
Mateo Fuentes	677455222	mfuentes@recursoshtelecom.com	113
Miguel Valverde	698364007	mvalverde@recursoshtelecom.com	114
Juan Pedro Muñoz	633259764	jpmuñoz@recursoshtelecom.com	115
Belén Quintanilla	683214756	bquintanilla@recursoshtelecom.com	116

DEPARTAMENTO DE COMERCIO			
Nombre	Teléfono	Correo electrónico	N.º Ext
Juan José Fernández	*654329876*	*jjfernandez@comerciohtelecom.com*	*210*
Ainara Bayona	685320147	abayona@comerciohtelecom.com	211
Lidia Domínguez	638907414	ldominguez@comerciohtelecom.com	211
José Luis Mayoral	677158962	jlmayoral@comerciohtelecom.com	213
Manuel Hidalgo	653002084	mhidalgo@comerciohtelecom.com	214
Ángela Ordoñez	600900837	aordoñez@comerciohtelecom.com	215
Agustín Salcedo	655358465	asalcedo@comerciohtelecom.com	216

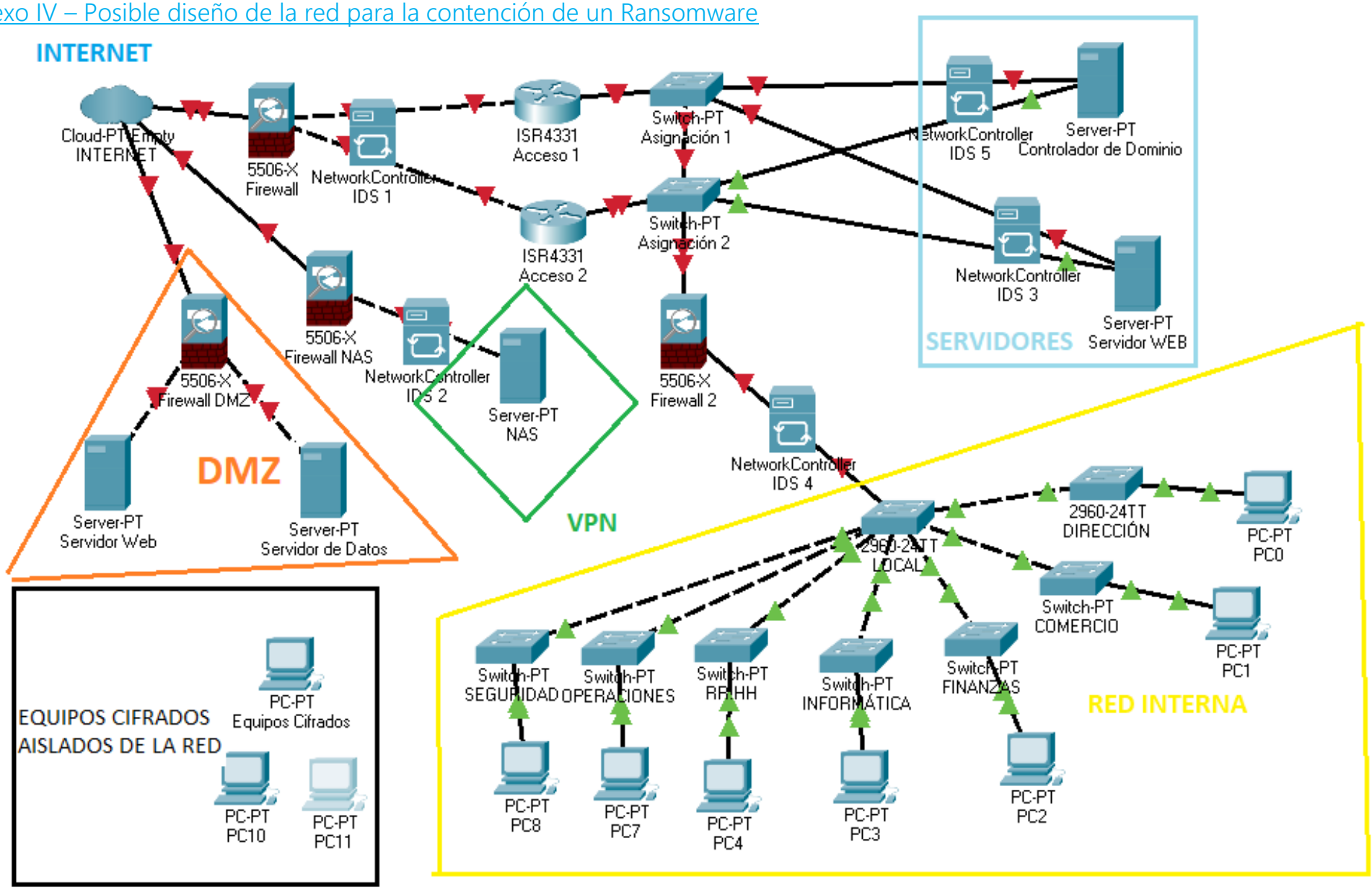
DEPARTAMENTO DE INFROMÁTICA			
Nombre	Teléfono	Correo electrónico	N.º Ext
Gonzalo Carvajal	*600754329*	*gcarvajal@informahtelecom.com*	*610*
Nicolás Medina	630258741	nmedina@informahtelecom.com	611
Belén Aguilera	698415655	baguilera@informahtelecom.com	612
Jesús Portillo	605741895	jportillo@informahtelecom.com	613
Inés Soriano	630789541	isoriano@informahtelecom.com	614
Jaime Cabañas	658074090	jcabañas@informahtelecom.com	615
Juan Trillo	679804709	jtillo@informahtelecom.com	616
Abril Torre	604084905	atorre@informahtelecom.com	617

DEPARTAMENTO DE SEGURIDAD			
Nombre	Teléfono	Correo electrónico	N.º Ext
Fernando Gutiérrez (Responsable ciberseguridad)	*678549005*	*fgutierrez@cibersechtelecom.com*	*310*
Leonor Herranz	659032415	lherranz@cibersechtelecom.com	311
Andrés Espejo	630245874	aespejo@cibersechtelecom.com	312
Rubén Sánchez (Responsable seguridad)	*629090861*	*rsanchez@sechtelecom.com*	*710*
Ernesto Fernandez	693254671	efernandez@sechtelecom.com	711
Rubén López	603425168	rlopez@sechtelecom.com	712
Juan Ávila	633592073	javila@sechtelecom.com	713
Jorge Martínez	917374500	jmartinez@sechtelecom.com	714

Anexo III – Checklist para la preparación del incidente

NIVEL	ALCANCE	CONTROL	
B	PRO	Equipo responsable	☐
B	PRO	Mejora continua	☐
B	PRO	Caducidad del plan de gestión de incidentes	☐
B	TEC	Detección del incidente	☐
B	TEC	Evaluación del incidente	☐
B	TEC	Comunicación interna del incidente	☐
A	TEC	Resolución de incidentes	☐
B	TEC	Tratamiento del registro del incidente	☐
B	PRO	Cumplimiento del RGPD	☐
B	TEC	Se han identificado los activos críticos	☐
B	PER	Comunicación externa del incidente	☐
B	PER	Concienciación y formación de los miembros de la organización	☐
B	PER - TEC	Se han realizado simulaciones	☐

Anexo IV – Posible diseño de la red para la contención de un Ransomware



Anexo V – Despliegue sonda SAT

El despliegue de la sonda SAT se realiza del siguiente modo:

1. Instalación de la sonda en el Organismo y configuraciones necesarias en la electrónica de red para enviar hacia la sonda el tráfico a analizar.
2. La conexión entre la sonda y el sistema central se realiza siempre de forma segura, a través del establecimiento de un túnel cifrado. Esta conexión puede realizarse a través de salida a Internet del Organismo adscrito o a través de una salida dedicada hacia Internet. El establecimiento de este túnel cifrado se inicia desde la sonda hacia el sistema central, no siendo necesaria ninguna infraestructura adicional por parte del organismo para el establecimiento de túneles cifrados.
3. La sonda se gestiona completamente desde el CCN-CERT, no siendo necesaria la realización de tareas de administración por parte del personal del Organismo. Eventualmente se solicitaría apoyo al Organismo en el caso que fuera necesaria la realización de tareas puntuales que no pudieran realizarse de manera remota.
4. De forma general, salvo que se pacte otra cosa, la sonda vigilará el tráfico de Internet de la red corporativa del Organismo y el de las DMZ's de servicios que el organismo ofrezca a Internet. Con los eventos recibidos se realiza una correlación avanzada de eventos en el sistema central, permitiendo la detección de ataques hacia los distintos organismos adscritos al sistema o la presencia de código dañino en estas redes.
5. La gestión, actualización y mantenimiento del sistema central está a cargo del CCN-CERT, que lleva a cabo tareas de administración, maduración de las reglas de detección e inclusión de nuevas funcionalidades y herramientas. De hecho, periódicamente se realiza la integración de numerosas reglas de detección, propias y externas, completando y ampliando la inteligencia del servicio y su capacidad de detección. Las reglas propias son generadas a partir de la información obtenida durante la investigación de otros incidentes de seguridad y a partir de la información recibida de otros organismos con los que se mantiene un intercambio de información referente a incidentes de seguridad.
6. Los usuarios pueden acceder en tiempo real a información relevante de los eventos generados por la sonda de su organismo, a informes periódicos y a la información de los incidentes de seguridad notificados a través de un portal accesible en Internet. Cada Organismo puede ver exclusivamente los eventos e informes relacionados con su red monitorizada.

Anexo VI - Checklist para la detección del incidente

NIVEL	ALCANCE	CONTROL	
A	TEC	Se ha instalado la sonda SAT	☐
A	TEC	Se ha implementado la solución microClaudia	☐
A	TEC	Se ha investigado el código dañino	☐
B	TEC	Se ha utilizado la herramienta noMoreRansom.org	☐
B	TEC	Se ha utilizado la herramienta ID Ransomware	☐
B	TEC	Se ha utilizado la herramienta noRansom	☐
B	TEC	Se ha utilizado la herramienta Emisoft	☐
B	TEC	Se ha utilizado la herramienta IDA Pro	☐
B	TEC	Se ha utilizado la herramienta Ghidra	☐
B	TEC	Se ha utilizado la herramienta Hybrid Analysis	☐
B	TEC	Se ha utilizado la herramienta Any Run	☐
B	TEC	Se ha utilizado la herramienta Virus Total	☐
B	TEC	Se ha utilizado la herramienta Triage	☐
B	TEC	Se ha utilizado la herramienta FileScan.io	☐

Anexo VII - Checklist para la mitigación del incidente

NIVEL	ALCANCE	CONTROL	
A	TEC	Se ha detectado el incidente	☐
A	TEC	Se ha rediseñado la red	☐
A	TEC	Se ha implementado un firewall	☐
A	TEC	Se han aislado los equipos afectados	☐
B	TEC	Se ha revisado que los equipos estén actualizados	☐
B	TEC	Se han actualizado los equipos	☐
B	TEC	Se han implementado parches en los equipos	☐
B	TEC	Se ha revisado el listado de usuarios dados de alta	☐
B	TEC	Se han eliminado los usuarios no deseados	☐

Anexo VIII - Checklist para la recuperación del incidente

NIVEL	ALCANCE	CONTROL	
A	PER – TEC	Se ha identificado el escenario del incidente	☐
A	TEC	Se han recuperado las copias de seguridad	☐
A	TEC	Se han aplicado herramientas de descifrado	☐
A	TEC	Se han recuperado las Shadow Volume Copy	☐
A	TEC	Se ha realizado un análisis forense	☐
A	TEC	Se han recuperado datos borrados mediante software forense	☐
A	TEC	Se han aislado los datos cifrados	☐
A	TEC	Se ha realizado el inventariado de los equipos afectados	☐
A	TEC	Se ha implantado la solución microClaudia	☐

Anexo IX - Checklist para la prevención del incidente

NIVEL	ALCANCE	CONTROL	
A	PER-TEC	Se han actualizado las políticas de seguridad	☐
B	TEC	Se ha deshabilitado la ejecución de scripts	☐
B	TEC	Se ha deshabilitado la ejecución de macros	☐
A	TEC	Se ha implementado una política de contraseñas	☐
B	TEC	Se ha implementado factor doble de autenticación (2FA)	☐
B	TEC	Se ha revisado el listado de usuarios dados de alta en el dominio	☐
B	PER	Se implementa un proceso de concienciación de los empleados	☐
B	PER	Se implementa un proceso de formación para los empleados	☐
A	TEC	Se ha implementado un firewall	☐
B	TEC	Se registra toda la actividad de la red	☐
B	TEC	Se monitoriza toda la actividad de la red	☐
A	TEC	Se han implantado medidas de seguridad (SIEM, IPs, Ids, etc.)	☐
A	TEC	Se han creado reglas de detección anti-spam	☐
A	TEC	Se ha implementado un sistema de copias de seguridad	☐
B	TEC	Se crean copias diarias de los equipos críticos	☐
A	TEC	Se han aislado los servidores de copias de seguridad	☐
B	TEC	Se crean más de una copia de seguridad para el mismo activo	☐
B	TEC	Se mantienen copias en formato papel de la información crítica de la organización	☐
A	TEC	Se realizan copias periódicas aisladas y desconectadas de la red	☐

Anexo X – Herramientas de investigación de código dañino

HERRAMIENTAS DE ANÁLISIS DE RANSOMWARE

noMoreRansom.org

https://www.nomoreransom.org/es/index.html

Mediante la herramienta *CryptoSheriff* nos permite identificar el tipo de ransomware que está afectando a nuestro equipo. A su vez, comprueba si existe una solución disponible. En el caso de existir, nos proporcionará una herramienta de descifrado.

Para ello, debemos subir uno de nuestros ficheros cifrados, de un tamaño no superior a 1MB a la página web de la herramienta, añadiendo las notas de rescate. La herramienta cotejará los datos introducidos en sus bases de datos y en caso de coincidir con alguno de los ransomware ya conocidos, nos proporcionará una herramienta de descifrado.

ID Ransomware

https://id-ransomware.malwarehunterteam.com/

Esta herramienta sirve para lo mismo que la anterior, identificar la familia de ransomware que ha afectado a nuestros equipos. Actualmente detecta un total de 1104 ransomware diferentes.

A diferencia de la herramienta noMoreRansom, esta no nos proporciona un método o herramienta de descifrado, sino que sólo nos identifica la familia del ransomware.

noRansom

https://noransom.kaspersky.com/

Proyecto de Kaspersky, nos ofrece algunas herramientas de descifrado para distintos tipos de ransomware.

El funcionamiento es similar a las herramientas anteriores; debemos acceder a la página web de la herramienta e introducir la extensión del archivo, el correo electrónico o cualquier otra información que nos aparezca en el mensaje del rescate.

Emisoft

https://www.emsisoft.com/en/ransomware-decryption/

Herramienta que nos ofrece distintas herramientas de descifrado para diferentes tipos de ransomware.

HERRAMIENTAS DE ANÁLISIS DE MALWARE (GENERAL)

IDA Pro

https://hex-rays.com/ida-pro/

IDA Pro es una herramienta especializada en ingeniería inversa de softwares maliciosos y en análisis de malware. Soporta una variedad de formatos ejecutables para diferentes procesadores y sistemas operativos.

Ghidra

https://ghidra-sre.org/

Ghidra es una herramienta de reversing de malware creada por la NSA.

Hybrid Analysis

https://www.hybrid-analysis.com/

Hybrid Analysis es una herramienta de análisis de malware que funciona con sandbox en línea. Estas sandbox permiten hacer pruebas con malware sin el uso de ningún software instalado.

Any Run

https://any.run/

Any Run es otro sandbox online para ejecutar malware y observar su funcionamiento mediante una página web. A su vez, la herramienta proporciona un análisis completo del malware.

VirusTotal

https://www.virustotal.com/gui/home/upload

VirusTotal proporciona el análisis de archivos y páginas web a través de antivirus. Incluye 55 antivirus y 61 motores de detección en línea.

Triage

https://tria.ge/

Triage es otro sandbox en línea que permite el análisis de malware.

FileScan.io

https://www.filescan.io/scan

FileScan.io es un sandbox de próxima generación que permite análisis de malware. Su tecnología de detección de amenazas adaptable permite la detección de malware *zero day* (día cero) y detección de Indicadores de Compromiso (IOCs).

Anexo XI – Listado de usuarios pertenecientes al dominio

LISTADO DE USUARIOS DADOS DE ALTA EN EL DOMINIO		
DEPARTAMENTO	*Nivel Privilego - Admin*	*NOMBRE*
DIR	10 – Sí	evillacampa@htelecom
DIR-INF	10 - Sí	gcarvajal@htelecom
DIR-SEC	10 – Sí	fgutierrez@htelecom
DIR-SEC	9 – Sí	rsanchez@htelecom
DIR-OP	8 – Sí	fcastiella@htelecom
DIR-FIN	8 – Sí	dramirez@htelecom
DIR-RR.HH	8 – Sí	clopez@htelecom
DIR-COM	8 - Sí	jjfernandez@htelecom
INF	8 - Sí	nmedina@htelecom
INF	8 – Sí	baguilera@htelecom
INF	8 - Sí	jportillo@htelecom
INF	8 – Sí	isoriano@htelecom
INF	8 – Sí	jcabañas@htelecom
INF	8 – Sí	jtillo@htelecom
INF	8 – Sí	atorre@htelecom
FIN	6 - No	hjaen@htelecom
FIN	6 – No	ccalderon@htelecom
FIN	6 – No	abalaguer@htelecom
FIN	6 – No	msandoval@htelecom
FIN	6 – No	fmartinez@htelecom

FIN	6 – No	ibenitez@htelecom
FIN	6 – No	dvalverde@htelecom
OP	6 - No	jcasal@htelecom
OP	6 – No	fllopis@htelecom
OP	6 - No	rsevilla@htelecom
OP	6 – No	acantero@htelecom
OP	6 - No	alucena@htelecom
OP	6 – No	mmateu@htelecom
OP	6 – No	fcarranza@htelecom
OP	6 – No	jcalvo@htelecom
OP	6 - No	sortiz@htelecom
OP	6 – No	mrequena@htelecom
RR.HH	6 – No	bvicens@htelecom
RR.HH	6 – No	cprieto@htelecom
RR.HH	6 – No	mfuentes@htelecom
RR.HH	6 – No	mvalverde@htelecom
RR.HH	6 – No	jpmuñoz@htelecom
RR.HH	6 – No	bquintanilla@htelecom
COM	6 – No	abayona@htelecom
COM	6 – No	ldominguez@htelecom
COM	6 – No	jlmayoral@htelecom
COM	6 – No	mhidalgo@htelecom
COM	6 – No	aordoñez@htelecom
COM	6 – No	asalcedo@htelecom

SEC	9 - Sí	lherranz@htelecom
SEC	9 - Sí	aespejo@htelecom
SEC	7 – No	efernandez@htelecom
SEC	7 – No	rlopez@htelecom
SEC	7 – No	javila@htelecom
SEC	7 – No	jmartinez@htelecom
Revisado por: Gonzalo Carvajal – Director Dep. Informática		Fecha: 8/5/2023

Anexo XII – Listado de equipos afectados

LISTADO DE EQUIPOS AFECTADOS			
EQUIPO	*DATOS*	*IMPACTO*	*ESTADO*
Windows 10 Dep. Comercio	Datos de clientes Datos financieros de la organización	Impacto bajo en la organización Ficheros cifrados	En proceso de descifrado, se ha obtenido una herramienta de descifrado.
		EJEMPLO	
Revisado por: Gonzalo Carvajal – Director Dep. Informática			Fecha: 8/5/2023

Anexo XIII – Checklist para la contención del incidente

NIVEL	ALCANCE	CONTROL	
B	TEC	Se han desconectado los cables de red de los equipos	☐
B	TEC	Se han desactivado las interfaces de red de los equipos	☐
B	TEC	Se ha comprobado si el proceso dañino está en ejecución	☐
B	TEC	Se ha realizado un volcado de memoria	☐
A	TEC	Se ha finalizado la ejecución del proceso dañino	☐
B	TEC	Se ha arrancado el equipo en Modo Seguro	☐
B	TEC	Se ha realizado una copia de seguridad de los equipos	☐
B	TEC	Las copias de seguridad han sido aisladas fuera de la red	☐
A	TEC	Se ha rediseñado la red de la organización	☐
A	TEC	Se ha implementado un firewall	☐
B	TEC	Se ha monitorizado el tráfico de la red	☐
A	TEC	Se ha implementado la solución microClaudia	☐