Política de Gestión de Incidentes de Seguridad de la Información

Forestal Collicura Limitada

Información del Documento

Versión	Fecha de Creación		Descripción
1.0	28-07-2023		Creación y primera versión del documento.

(*) La última versión sustituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los efectos.

Tabla de contenido

1. *Introducción*

La presente política entrega los lineamientos bases para mantener un Sistema de Gestión de Incidentes de Seguridad de la información en **FORESTAL COLLICURA LIMITADA,** a través de un modelo propuesto, el cual está concebido para que se puedan integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren.

2. *Objetivo*

El objetivo principal de la Gestión de Incidentes de seguridad de la información en **FORESTAL COLLICURA LIMITADA,** es tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad.

3. *Alcance*

Esta política se aplica a todo el personal con contrato parcial, tiempo completo, a honorarios, y estudiante en Práctica de **FORESTAL COLLICURA LIMITADA.** Específicamente a los administradores de TI y al equipo de respuesta a incidentes que **FORESTAL COLLICURA LIMITADA** debe implementar.

4. *Definiciones*

Incidente de seguridad de la información: Interrupción o alteración del proceso normal de seguridad de los activos de información o una situación de fallas en seguridad de la información con probabilidad significativa de comprometer la confidencialidad, integridad y disponibilidad de la información de **FORESTAL COLLICURA LIMITADA.**

Incidente de ciberseguridad: Interrupción o alteración del proceso normal de seguridad de los activos de información digitales, la infraestructura tecnológica, los componentes lógicos de la información y las interacciones en el ciberespacio con probabilidad significativa de comprometer las operaciones de **FORESTAL COLLICURA LIMITADA.**

SOC: Security Operation Center. Central de seguridad informática de **FORESTAL COLLICURA LIMITADA**. Su labor es prevenir, monitorear y controlar la seguridad en las redes y en Internet. Participar en el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, gestión de riesgos y alertas de amenazas informáticas.

SIEM: Security Information and Event Management. Sistema que centraliza el almacenamiento y la interpretación de los datos relevantes de seguridad. De esta forma, permite un análisis de la situación en múltiples ubicaciones desde un punto de vista unificado que facilita la detección de tendencias y patrones no habituales. La mayoría de los sistemas SIEM funcionan desplegando múltiples agentes de recopilación que recopilan eventos relacionados con la seguridad.

IDS: Un sistema de detección de intrusiones o IDS es un programa de detección de accesos no autorizados a un computador o a una red.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, las anomalías que pueden ser indicio de la presencia de ataques y falsas alarmas.

IPS: Un sistema de prevención de intrusos (o por sus siglas en inglés IPS) es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

IOA: Indicadores de ataque son las señales que indican una actividad potencialmente maliciosa en curso o un patrón de comportamiento que podría indicar un ataque en sus etapas tempranas. Para una detección más proactiva podemos indicar los siguientes:

- Comportamiento en tiempo real

- Metadatos de ejecución de código
- Bibliotecas de enlaces dinámicos (DLL)
- Secuencia de eventos
- Acciones realizadas
- Comportamiento del usuario en relación con la amenaza digital
- TTps vinculados a datos hostiles como malware, utilizados en un ataque
- Componentes persistentes y sigilosos utilizados en un ataque

IOC: Indicadores de compromiso

Los IOC son señales específicas que indican que un sistema o red de que ha sido comprometidos. Estos indicadores se basan en firmas y patrones conocidos asociados con malware virus u otras amenazas previamente identificadas por otros profesionales de la materia. Los IOC se utilizan para identificar actividades maliciosas que ya han sido detectadas y se encuentran en bases de datos públicas. Ejemplos comunes de los IOC son:

- Nombre de Archivo.
- Hashes (MD5 – SHA1 – SHA256).
- Conexión a un servidor C2 (Command and Control).
- Direcciones IPs.
- Dominios.
- Herramientas.
- Registros de Eventos.
- Valores de Claves de Registro.

5. Modelo de Gestión de Incidentes

5.1 Preparación

Esta primera etapa dentro del ciclo de gestión de incidentes busca prevenir incidentes de seguridad y gestionar las vulnerabilidades, asegurando que los sistemas, redes, y aplicaciones sean lo suficientemente seguros.

Es responsabilidad de la organización implementar un Security Operation Center (SOC) que pueda velar por la disposición de los recursos de atención de incidentes y las herramientas necesarias para cubrir las demás etapas del ciclo de vida de incidentes.

5.1.1 Gestión de parches de seguridad

Se deben seguir los lineamientos de la política de "Gestión de vulnerabilidades" para la identificación, adquisición, prueba e instalación de los parches.

5.1.2 Aseguramiento de plataforma

- Se debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos.
- Se deben revisar configuraciones por default (usuarios, contraseñas y archivos compartidos).
- Los servidores deben tener habilitados sus sistemas de auditoría para permitir el login de eventos.
- Para más detalle ver: "Política de control de acceso".
- **FORESTAL COLLICURA LIMITADA** debe mantener un control diario de los IOA (indicadores de Ataque).

5.1.3 Seguridad en redes

Debe existir una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como firewalls, deben ser revisadas continuamente. Las firmas y actualizaciones de dispositivos como IDS o IPS deben encontrarse al día. Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus logs deben ser enviados para su respectivo análisis en el SIEM.

5.1.4 Prevención de código malicioso

Todos los equipos de la infraestructura (servidores, como equipos de usuario) deben tener activo un antivirus, antimalware con las firmas de actualización al día.

5.1.5 Recursos para el análisis de incidentes

- Tener un listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.
- Contar con un diagrama de red para tener la ubicación rápida de los recursos existentes.
- Una línea base de Información de: Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios). Esta información siempre debe estar actualizada para poder conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente.
- Se debe tener un análisis del comportamiento de red estándar; en este es recomendable incluir: puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.

5.2 Detección, evaluación y análisis

5.2.1 Análisis

Las actividades de análisis del incidente involucran otra serie de componentes, es recomendable tener en cuenta los siguientes:

- Tener conocimientos de las características normales a nivel de red y de los sistemas.
- Considerar los IOC y los IOA para análisis de todos los procesos de ataques detectados.

- Los administradores de TI deben tener conocimiento total sobre los comportamientos de la Infraestructura que están administrando.
- Toda información que permita realizar análisis al incidente debe estar centralizada (Logs de servidores, redes, aplicaciones).
- Es importante efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento anormal y poder identificar de manera más fácil la causa del incidente.
- Para un correcto análisis de un incidente debe existir una única fuente de tiempo (Sincronización de Relojes) ya que esto facilita la correlación de eventos y el análisis de información.
- Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.
- Crear matrices de diagnóstico e información para los administradores menos experimentados.

5.2.2 Evaluación y priorización

Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto que nos proporciona la tabla del Framework Magerit. La cual determinará la prioridad que se le debe dar al incidente.

5.2.3 Tiempos de respuesta

Para la atención de incidentes de seguridad se han establecido tiempos máximos de atención de estos, con el fin de atender adecuadamente los incidentes de acuerdo a su criticidad e impacto. Los tiempos expresados en la siguiente tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el

incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

Nivel de impacto	Tiempo de respuesta Máximo
Bajo	**1 hora**
Medio	**40 minutos**
Alto	**20 minutos**
Crítico	**10 minutos**

5.2.4 Clasificación de incidentes de seguridad de la información

La clasificación de incidentes que afectan a la confidencialidad, integridad o disponibilidad de los activos de información se debe realizar en base a la tabla del **Anexo A.2**

5.2.5 Declaración y notificación de incidentes

Cualquier usuario, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad, o correos sospechosos deberá notificarlo mediante correo a las casilla: compliance@collicura.cl

El analista SOC debe identificar el tipo de incidente (de acuerdo a la tabla de clasificación de incidentes). Analizará si el incidente reportado corresponde a un incidente de seguridad de la información o está relacionado con requerimientos propios de la infraestructura de TI, y debe escalarlo a quien corresponda. El analista SOC es el encargado de realizar el seguimiento del incidente hasta su cierre definitivo.

Si el incidente de seguridad es identificado por otra línea diferente a un usuario de **FORESTAL COLLICURA LIMITADA**, a través de los elementos de detección o

administradores de TI, este debe ser notificado directamente a la persona correspondiente encargada de su resolución. Adicionalmente se debe notificar al Analista SOC sobre la presentación del incidente de seguridad para que realice la documentación respectiva y esté atento al seguimiento y desarrollo de este.

El ingeniero SOC igualmente debe estar involucrado desde el inicio del ciclo de vida del incidente y se encarga de coordinar y asignar las actividades con las partes involucradas en la resolución. Estos últimos se encargan de solicitar el apoyo a las personas involucradas con el proceso con el fin de la correcta ejecución de actividades que den solución al incidente.

El ingeniero y jefe SOC tendrán la potestad para decidir sobre las acciones que se deban ejecutar ante la presencia de un incidente de seguridad y de notificar a la alta gerencia de **FORESTAL COLLICURA LIMITADA**.

5.3 Contención, erradicación y recuperación

Es de vital importancia tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a nuestra infraestructura tecnológica y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

Contención: Esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI. Para facilitar esta tarea el SOC debe contar con un playbook de respuesta ante incidentes para poder tomar decisiones de contención previamente definidas.

Erradicación y Recuperación: Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente, posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual los administradores de TI deben restablecer la

funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

Durante el proceso de atención de incidentes de seguridad específicamente en la fase de "Contención, Erradicación y Recuperación" se puede hacer necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) en el caso que un incidente afecte gravemente a un determinado sistema.

5.4 Actividades Post-incidente

Una vez resuelto el incidente se debe generar el reporte apropiado, existen lecciones aprendidas, se establecen medidas tecnológicas, disciplinarias y penales de ser necesarias, así como el registro en la base de conocimiento para alimentar los indicadores.

5.4.1 Lecciones aprendidas

Mantener un proceso de "lecciones aprendidas" después de un incidente grave, y periódicamente después de los incidentes menores, es primordial para la mejora de las medidas de seguridad y el proceso de gestión de incidentes.
Mantener un adecuado registro de lecciones aprendidas permite conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Los procedimientos documentados.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Acciones correctivas pueden prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

6. Responsabilidades

Usuarios: Responsables de notificar al equipo de respuesta ante incidentes cualquier situación anómala en los sistemas de **FORESTAL COLLICURA LIMITADA**, indicio de ataque o incidente de seguridad de la información.

Analista SOC: Es el encargado de recibir las solicitudes por parte de los usuarios sobre posibles incidentes, debe registrarlos, realizando una clasificación del tipo de incidente e impacto, además de escalarlos a la personas encargadas de su resolución.

Ingeniero SOC: Es responsable de realizar un análisis profundo de los incidentes de seguridad. Se debe coordinar con el resto de las áreas de TI para comprender la naturaleza y el alcance del incidente, colaborando en idear formas de mitigar o remediar el incidente.

Administrador de plataforma TI: Persona encargada de configurar y mantener un activo informático. Debe ser notificado por el **Ingeniero SOC** sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar el incidente de seguridad. Este debe documentar y notificar al **Ingeniero SOC** sobre el incidente y la solución del mismo respetando los tiempos de resolución establecidos en esta política. Los administradores de plataforma TI que no cumplan estas instrucciones se arriesgan a sanciones administrativas dependiendo de la gravedad de la omisión.

Administrador de sistemas de seguridad: Encargados de configurar y mantener un activo informático relacionado con la seguridad de la plataforma ej: Firewall, Sistemas de Prevención de Intrusos, Routers, Sistemas de Gestión y Monitoreo. Debe ser notificado por el **Ingeniero SOC** sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al **Ingeniero SOC** sobre el incidente y la solución del mismo respetando los tiempos de resolución establecidos en esta política. Los administradores de plataforma TI que no cumplan estas instrucciones se arriesgan a sanciones administrativas dependiendo de la gravedad de la omisión.

Jefe SOC: Responde a las consultas sobre los incidentes de impacto **ALTO** y **CRÍTICO**, es el encargado de revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a la alta gerencia. El Jefe SOC tiene la capacidad de convocar la participación de otros funcionarios de **FORESTAL COLLICURA LIMITADA** cuando el incidente lo amerita y gatillar planes de contingencia y/o continuidad.

7. Sanciones

La Seguridad de la Información y la Ciberseguridad resguardan los activos más importantes de **FORESTAL COLLICURA LIMITADA**, por lo cual la omisión, no ejecución o desinterés por parte de las personas encargadas, generan un desmedro en la calidad de los servicios y suponen un alto riesgo operacional y de reputación de **FORESTAL COLLICURA LIMITADA**, por lo cual estos actos deben traer consigo sanciones administrativas por parte de **FORESTAL COLLICURA LIMITADA**.
Estas sanciones deben quedar reflejadas en el reglamento interno de **FORESTAL COLLICURA LIMITADA**.

8. Documentación de referencia

"Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información - MINTIC"

8.1 Documentos relacionados

- Política de control de acceso
- Política de gestión de vulnerabilidades
- Reglamento Interno

Anexo A

1. ***Tabla de impacto de acuerdo a Magerit***

NIVEL DE IMPACTO	IMPACTOS POTENCIALES DEL CIBERINCIDENTE	CRITERIOS / POSIBLES CONSECUENCIAS
CRÍTICO	**Imagen y reputación:** problemas en las relaciones con clientes, proveedores y otros stakeholders claves del sector e impacto negativo en medios de comunicación.	El número de clientes, proveedores y otros *stakeholders* claves del sector que se ven afectados por la perturbación del servicio es extremadamente alto.
		Daños de reputación elevados y cobertura continua en medios de comunicación nacionales e internacionales.
	Estrategia: poner en riesgo la consecución de uno o más objetivos de **FORESTAL COLLICURA LIMITADA**.	El alcance del impacto afecta a la consecución de más del 90% de los objetivos de **FORESTAL COLLICURA LIMITADA**.

	<u>Cumplimiento legal:</u> incumplimiento de legislación en materia de datos de carácter personal e incumplimiento de otras obligaciones legales (leyes y regulaciones específicas) que le sean de aplicación a la **FORESTAL COLLICURA LIMITADA**.	El ciberincidente probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación.
	<u>Gestión responsable y sostenibilidad:</u> incumplimiento de compromisos de gestión responsable y sostenible asumidos voluntariamente por **FORESTAL COLLICURA LIMITADA**.	El impacto deriva en un incumplimiento extremadamente grave de los compromisos adquiridos voluntariamente por **FORESTAL COLLICURA LIMITADA** con los distintos grupos de interés.
	<u>Presupuesto y costes:</u> causar elevados cambios en el presupuesto o pérdidas excepcionalmente elevadas de muy alto valor económico.	El impacto deriva en un aumento del coste del servicio de más del 90%.
		El impacto genera una pérdida de beneficios de más del 90% respecto a los del año anterior.

	Operación: causar interrupciones en las actividades de la empresa pudiendo ocasionar impacto en terceros.	El alcance del impacto afecta a más del 90% de los servicios prestados por la empresa.
		El impacto ocasiona una interrupción del/los servicio/s de más de 8 horas.
		El impacto ocasiona una interrupción del/los servicio/s de más de 24 horas.
	Satisfacción: causar incumplimientos en plazos de entrega o prestación de servicios y quejas de los stakeholders que puedan derivar en pérdida de fidelización de la cartera de clientes o de proveedores.	El impacto ocasiona un incumplimiento extremadamente grave de los plazos de entrega establecidos.
		El impacto ocasiona pérdidas de más del 90% de la cartera de clientes o de proveedores.
		El impacto ocasiona un incumplimiento muy grave de los plazos de entrega establecidos.
		El ciberincidente probablemente afecte gravemente a un grupo de individuos.

	Seguridad para las personas y/o instalaciones: causar daños y perjuicios a las personas o a las instalaciones corporativas.	Las instalaciones corporativas se han visto afectadas de forma extremadamente grave.
		El alcance del impacto afecta entre el 75% y el 90% de los servicios prestados por **FORESTAL COLLICURA LIMITADA.**
	Seguridad para los sistemas: causar daños en los sistemas de información en los que están soportados los servicios prestados por la empresa o en los que se almacena información necesaria para la correcta operativa de los servicios.	El impacto afecta a más del 75% de los sistemas de información de **FORESTAL COLLICURA LIMITADA**.
ALTO	**Imagen y reputación:** problemas en las relaciones con clientes, proveedores y otros stakeholders claves del	El número de clientes, proveedores y otros stakeholders claves del sector que se ven afectados por la perturbación del servicio es alto.

	sector e impacto negativo en medios de comunicación.	Daños de reputación de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
	Estrategia: poner en riesgo la consecución de uno o más objetivos de empresa.	El alcance del impacto afecta a la consecución de entre el 51% y el 75% de los objetivos de la empresa.
	Cumplimiento legal: incumplimiento de legislación en materia de datos de carácter personal e incumplimiento de otras obligaciones legales (leyes y regulaciones específicas) que le sean de aplicación a **FORESTAL COLLICURA LIMITADA**.	El ciberincidente probablemente cause un incumplimiento grave de una ley o regulación.
	Gestión responsable y sostenibilidad: incumplimiento de compromisos de gestión responsable y sostenible asumidos voluntariamente por	El impacto deriva en un incumplimiento grave de los compromisos adquiridos voluntariamente por **FORESTAL COLLICURA LIMITADA** con los distintos grupos de interés.

	FORESTAL COLLICURA LIMITADA.	El impacto deriva en un aumento del coste del servicio de entre el 51% y el 75%.
	<u>Presupuesto y costes:</u> causar elevados cambios en el presupuesto o pérdidas excepcionalmente elevadas de muy alto valor económico.	El impacto genera una pérdida de beneficios de entre el 51% y el 75% respecto a los del año anterior.
	<u>Operación:</u> causar interrupciones en las actividades de **FORESTAL COLLICURA LIMITADA** pudiendo ocasionar impacto en terceros.	El alcance del impacto afecta entre el 51% y el 75% de los servicios prestados por **FORESTAL COLLICURA LIMITADA.**
	<u>Satisfacción:</u> causar incumplimientos en plazos de entrega o prestación de servicios y quejas de los stakeholders que puedan derivar en pérdida de fidelización de la cartera de clientes o de proveedores.	El impacto ocasiona un incumplimiento grave de los plazos de entrega establecidos.
		El impacto ocasiona pérdidas de entre el 51% y el 75% de la cartera de clientes o de proveedores.
		El ciberincidente probablemente afecte a un grupo de individuos.

	<u>Seguridad para las personas y/o instalaciones:</u> causar daños y perjuicios a las personas o a las instalaciones corporativas.	Las instalaciones corporativas se han visto gravemente afectadas.
	<u>Seguridad para los sistemas:</u> causar daños en los sistemas de información en los que están soportados los servicios prestados por **FORESTAL COLLICURA LIMITADA** o en los que se almacena información necesaria para la correcta operativa de los servicios.	El impacto afecta a más del 50% de los sistemas de información de **FORESTAL COLLICURA LIMITADA**.
MEDIO	**<u>Imagen y reputación:</u>** problemas en las relaciones con clientes, proveedores y otros stakeholders claves del sector e impacto negativo en medios de comunicación.	El número de clientes, proveedores y otros stakeholders claves del sector afectados por la perturbación del servicio es importante.
		Daños de reputación apreciables, con eco mediático (amplia cobertura en medios de comunicación).
	<u>Estrategia:</u> poner en riesgo la consecución de uno o más objetivos de **FORESTAL COLLICURA LIMITADA.**	El alcance del impacto afecta a la consecución de entre el 21% y el 50% de los objetivos de

		FORESTAL COLLICURA LIMITADA.
	<u>Cumplimiento legal:</u> incumplimiento de legislación en materia de datos de carácter personal e incumplimiento de otras obligaciones legales (leyes y regulaciones específicas) que le sean de aplicación a la empresa.	El ciberincidente probablemente sea causa de incumplimiento leve o técnico de una ley o regulación.
	<u>Gestión responsable y sostenibilidad:</u> incumplimiento de compromisos de gestión responsable y sostenible asumidos voluntariamente por la **FORESTAL COLLICURA LIMITADA.**	El impacto deriva en un incumplimiento importante de los compromisos adquiridos voluntariamente por **FORESTAL COLLICURA LIMITADA** con los distintos grupos de interés.
	<u>Presupuesto y costes:</u> causar elevados cambios en el presupuesto o pérdidas excepcionalmente elevadas de muy alto valor económico.	El impacto deriva en un aumento del coste del servicio de entre el 21% y el 50%.
		El impacto genera una pérdida de beneficios de entre el 21% y el 50% respecto a los del año anterior.

	<u>Operación:</u> causar interrupciones en las actividades de **FORESTAL COLLICURA LIMITADA** pudiendo ocasionar impacto en terceros.	El alcance del impacto afecta entre el 21% y el 50% de los servicios prestados por **FORESTAL COLLICURA LIMITADA**.
	<u>Satisfacción:</u> causar incumplimientos en plazos de entrega o prestación de servicios y quejas de los stakeholders que puedan derivar en pérdida de fidelización de la cartera de clientes o de proveedores.	El impacto ocasiona un incumplimiento alto de los plazos de entrega establecidos.
		El impacto ocasiona pérdidas de entre el 21% y el 50% de la cartera de clientes o de proveedores.
		El ciberincidente probablemente afecte a un individuo.
	<u>Seguridad para las personas y/o instalaciones:</u> causar daños y perjuicios a las personas o a las instalaciones corporativas.	Las instalaciones corporativas se han visto afectadas de forma importante.

	Seguridad para los sistemas: causar daños en los sistemas de información en los que están soportados los servicios prestados por **FORESTAL COLLICURA LIMITADA** o en los que se almacena información necesaria para la correcta operativa de los servicios.	El impacto afecta entre el 21% y el 50% de los sistemas de información de **FORESTAL COLLICURA LIMITADA**.
BAJO	**Imagen y reputación:** problemas en las relaciones con clientes, proveedores y otros stakeholders claves del sector e impacto negativo en medios de comunicación.	El número de clientes, proveedores y otros stakeholders claves del sector que se ven afectados por la perturbación del servicio es mínimo.
		Daños de reputación puntuales, sin eco mediático.
	Estrategia: poner en riesgo la consecución de uno o más objetivos de **FORESTAL COLLICURA LIMITADA**.	El alcance del impacto afecta a la consecución de hasta un 20% de los objetivos de **FORESTAL COLLICURA LIMITADA**.
	Cumplimiento legal: incumplimiento de legislación en materia de datos de carácter personal e incumplimiento de otras obligaciones legales (leyes y regulaciones específicas) que	El ciberincidente pudiera causar el incumplimiento leve o técnico de una ley o regulación.

	le sean de aplicación a la **FORESTAL COLLICURA LIMITADA**.	
	Gestión responsable y sostenibilidad: incumplimiento de compromisos de gestión responsable y sostenible asumidos voluntariamente por la empresa.	El impacto deriva en un incumplimiento menor de los compromisos adquiridos voluntariamente por **FORESTAL COLLICURA LIMITADA** con los distintos grupos de interés.
	Presupuesto y costes: causar elevados cambios en el presupuesto o pérdidas excepcionalmente elevadas de muy alto valor económico.	El impacto deriva en un aumento del coste del servicio de hasta un 20%.
		El impacto genera una pérdida de beneficios de hasta el 20% respecto a los del año anterior.
	Operación: causar interrupciones en las actividades de **FORESTAL COLLICURA LIMITADA** pudiendo ocasionar impacto en terceros.	El alcance del impacto afecta hasta el 20% de los servicios prestados por **FORESTAL COLLICURA LIMITADA**.

	<u>Satisfacción:</u> causar incumplimientos en plazos de entrega o prestación de servicios y quejas de los stakeholders que puedan derivar en pérdida de fidelización de la cartera de clientes o de proveedores.	El impacto ocasiona un incumplimiento leve de los plazos de entrega establecidos.
		El impacto ocasiona pérdidas de hasta el 20% de la cartera de clientes o de proveedores.
	<u>Seguridad para las personas y/o instalaciones:</u> causar daños y perjuicios a las personas o a las instalaciones corporativas.	El ciberincidente pudiera causar molestias a un individuo.
		Las instalaciones corporativas se han visto afectadas de forma leve.
	<u>Seguridad para los sistemas:</u> causar daños en los sistemas de información en los que están soportados los servicios prestados por **FORESTAL COLLICURA LIMITADA** o en los que se almacena información necesaria para la correcta operativa de los servicios.	El impacto afecta hasta un 20% de los sistemas de información de **FORESTAL COLLICURA LIMITADA**.

2. Clasificación de Incidentes de Ciberseguridad de acuerdo con "Enisa"

Matriz de clasificación de incidentes		
Clase de Incidente	**Tipo de Incidente**	**Descripción**
Contenido Abusivo	Pornografía Infantil – Sexual – Violencia	Pornografía infantil, glorificación de la violencia, otros.
	Spam	«Correo masivo no solicitado», lo que significa que el destinatario no ha otorgado permiso verificable para que el mensaje sea enviado y además el mensaje es enviado como parte de una grupo masivo de mensajes, todos teniendo un contenido similar
	Difamación	Desacreditación o discriminación de alguien

Código Malicioso	Malware, Virus, Gusanos, Troyanos, spyware, Dialler, rootkit	Software que se incluye o inserta intencionalmente en un sistema con propósito dañino. Normalmente, se necesita una interacción del usuario para activar el código.
Recopilación de Información	Scanning	Ataques que envían solicitudes a un sistema para descubrir puntos débiles. Se incluye también algún tipo de proceso de prueba para reunir información sobre hosts, servicios y cuentas. Ejemplos: fingerd, consultas DNS, ICMP, SMTP (EXPN, RCPT, …), escaneo de puertos.
	Sniffing	Observar y registrar el tráfico de la red (escuchas telefónicas o redes de datos).
	Ingeniería Social	Recopilación de información de un ser humano de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).
Intentos de Intrusión	Intentos de acceso	Múltiples intentos de inicio de sesión (adivinar / descifrar contraseñas, fuerza bruta).

	Explotación de vulnerabilidades conocidas	Un intento de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas que ya cuentan con su clasificación estandarizada CVE (por ejemplo, el búfer desbordamiento, puerta trasera, secuencias de comandos cruzadas, etc.).
	Nueva Firma de Ataque	Un intento de usar un exploit desconocido.
Intrusión	Compromiso de Cuenta Privilegiada	Un compromiso exitoso de un sistema o aplicación (servicio). Esto puede haber sido causado de forma remota por una vulnerabilidad conocida o nueva, pero también por un acceso local no autorizado. También incluye ser parte de una botnet.
	Compromiso de Cuenta sin privilegios	
	Compromiso de Aplicación, Bot	
Disponibilidad	Ataque de denegación de servicio (DoS / DDoS)	Con este tipo de ataque, un sistema es bombardeado con tantos paquetes que las operaciones se retrasan o el sistema falla. Algunos ejemplos DoS son ICMP e inundaciones SYN, ataques de teardrop y bombardeos de mail's. DDoS a menudo se basa en ataques DoS que se originan en botnets, pero también existen otros

	Sabotaje	escenarios como Ataques de amplificación DNS. Sin embargo, la disponibilidad también puede verse afectada por acciones locales (destrucción, interrupción del suministro de energía, etc.), fallas espontáneas o error humano, sin mala intención o negligencia.
	Intercepción de información	
Información de seguridad de contenidos	Acceso no autorizado a la información	Además de un abuso local de datos y sistemas, la seguridad de la información puede estar en peligro por una cuenta exitosa o compromiso de la aplicación. Además, son posibles los ataques que interceptan y acceden a información durante la transmisión (escuchas telefónicas, spoofing o secuestro). El error humano / de configuración / software también puede ser la causa.
	Modificación no autorizada de la información	
Fraude	Phishing	Enmascarado como otra entidad para persuadir al usuario a revelar una credencial privada.
	Derechos de Autor	Ofrecer o instalar copias de software comercial sin licencia u otro materiales protegidos por derechos de autor.

	Uso no autorizado de recursos	Usar recursos para fines no autorizados, (por ejemplo, el uso del correo electrónico para participar en cartas de cadena de ganancias ilegales) o esquemas piramidales).
	Falsificación de registros o identidad	Tipo de ataques en los que una entidad asume ilegítimamente la identidad de otro para beneficiarse de ello.
Vulnerable	Sistemas y/o softwares Abiertos	Sistemas «Open Resolvers», impresoras abiertas a todo el mundo, vulnerabilidades aparentes detectadas con nessus u otros aplicativos, firmas de virus no actualizadas, etc.
Otros	Todos los incidentes que no encajan en alguna de las otras categorías dadas	Si la cantidad de incidentes en esta categoría aumenta, es un indicador de que el esquema de clasificación debe ser revisado.
Test	Para pruebas	Producto de pruebas de seguridad controladas e informadas