Servicios Gestionados de Seguridad | Brochure

Respuesta a Incidentes de Seguridad (CSIRT)

Respuesta a Incidentes de Seguridad

Con el aumento de los ataques cibernéticos en un escenario de amenazas complejo, una organización debe responder rápidamente y estar preparada para accionar en todas las situaciones.

La capacidad de una organización para responder rápidamente ante un incidente de seguridad es crucial para limitar el impacto del ataque, minimizando los daños a la reputación y las consecuencias legales. Las organizaciones necesitan contener el incidente y recuperarse inmediatamente. En muchos casos, los daños de un incidente cibernético aumentan debido a retrasos y errores en el tratamiento del incidente. La experiencia en reconocer los indicadores de compromiso de un ataque cibernético y la respuesta ante incidentes son campos altamente especializados que exigen que las personas trabajen continuamente en este espacio, lo que no es posible con un equipo contratado por media jornada. Como resultado, muchas organizaciones no cuentan con un equipo interno de respuesta ante incidentes, pero en su lugar, contratan proveedores externos, como NTT.

La Identificación, contención, erradicación, remediación y registro de lecciones aprendidas son partes del proceso de respuesta ante incidentes. En el servicio de CSIRT, nuestros especialistas preparan un plan de respuestas ante incidentes de acuerdo con el negocio, además de actuar de forma rápida y eficiente ante la presencia de un incidente, realizando todo el proceso en conjunto con el cliente y dando apoyo antes, durante y después de las crisis.

Además de los diferentes niveles de SLA y horas de servicio, NTT también realiza una evaluación del entorno del cliente al inicio del servicio para garantizar que el equipo de respuesta ante incidentes cuente con toda la información pertinente, lo que acelera las etapas iniciales.

CSIRT

	Silver	Gold	Platinum
Horas disponibles	80	120	240
Tiempo de respuesta remoto	4 horas	2 horas	2 horas

Respuesta a Incidentes de Seguridad

Las horas de servicio disponibles pueden y deben ser utilizadas en actividades previas de preparación de la respuesta ante incidentes a través de las siguientes actividades:

Desarrollo de un plan de respuesta ante incidentes	Desarrollo de la estructura exigida por la organización para operar de forma eficaz en caso de que ocurra un incidente.
Análisis de brechas de un plan de respuesta ante incidentes	**Revisión de la documentación de respuesta ante** incidentes de la organización, elaboración de un informe de evaluación con análisis de brechas, usando las mejores prácticas de negocios y estándares.
Análisis de plan de respuestas ante incidentes	**Desarrollo de escenarios de análisis específicos para la** organización, de acuerdo con el área de actuación, y la realización de ejercicios con un equipo de respuesta ante incidentes interno del cliente para evaluar cómo responde ante incidentes.
Evaluación del compromiso	**Evaluación del entorno del cliente en cuanto a la presencia** de la actividad de violación y detección de amenazas persistentes. Identificación de IOCs, artefactos de malware o actividades maliciosas de tráfico de red.
Desarrollo de Runbook de respuesta ante incidentes	Guía detallada sobre cómo responder a ataques muy específicos, como ransomware, malware, ataques de denegación de servicio, etc.

Nuestro CSIRT entrega:

- SOC 24x7 para respuestas ante incidentes.
- Manejo de conformidades con evidencias.
- Implementación remota de herramientas de respuesta ante incidentes.
- Integración con los servicios gestionados de seguridad de NTT para entrega de valor agregado.
- Análisis forense digital especializado.
- Equipo dedicado de ingeniería reversa de malware.
- Plena colaboración con los equipos del cliente.

En caso de un incidente de seguridad, el servicio brindará gestión de incidentes, contención y soporte forense para ayudar a mitigar el incidente. El equipo NTT CSIRT actúa en:

- Mitigación del Incidente
- Contención
- Informes de la situación
- Erradicación de la amenaza
- Recuperación


NTT DATA