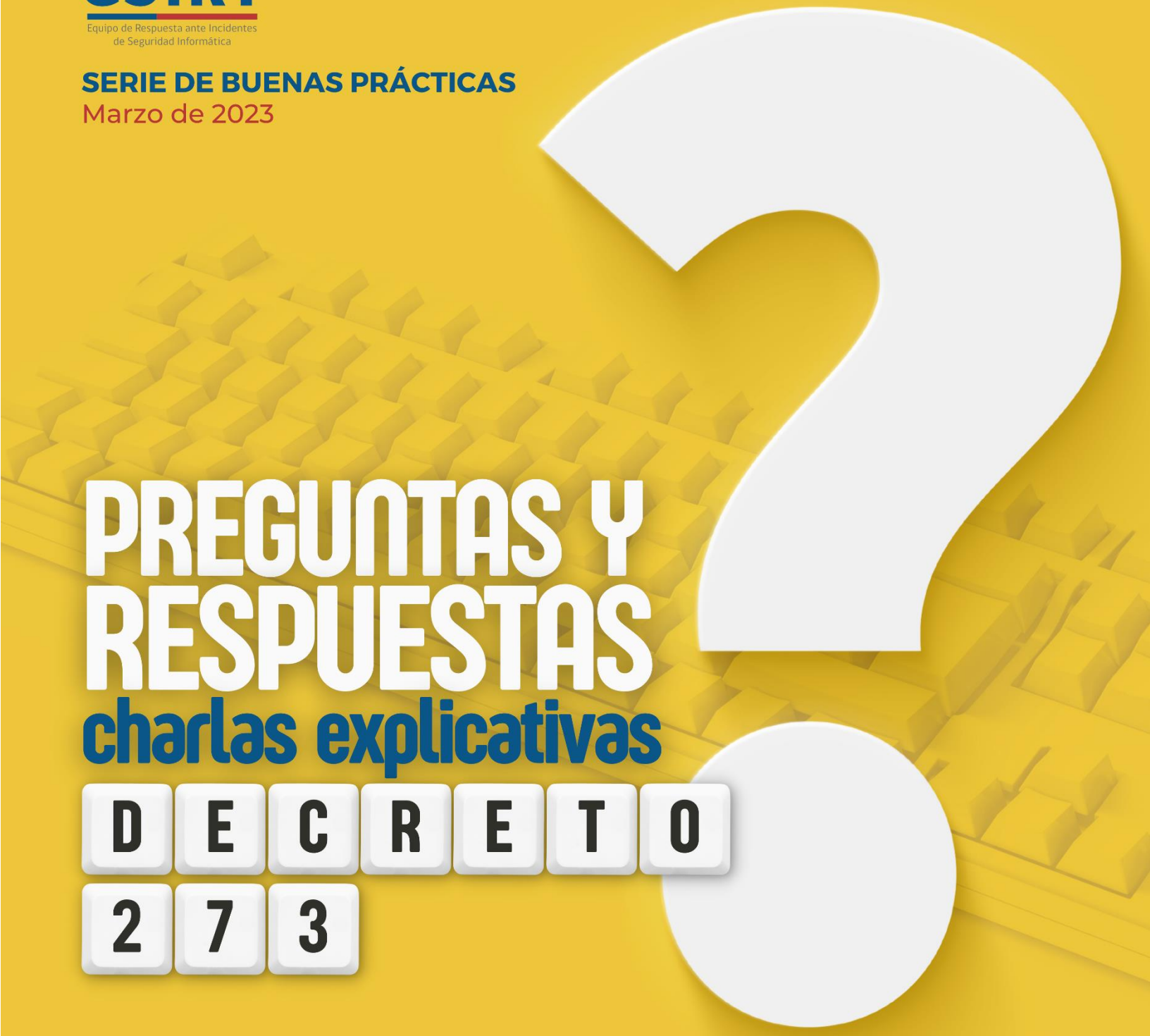
CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

SERIE DE BUENAS PRÁCTICAS

Marzo de 2023



PREGUNTAS Y RESPUESTAS

charlas explicativas

DECRETO 273

www.csirt.gob.cl

ÍNDICE

1. Preguntas sobre cuándo reportar y a quién..... 2
2. Preguntas sobre la necesidad de notificar en tres horas 5
3. Otras preguntas no relacionadas con el Decreto 273 de 2022..... 6

Dirección Ingrid Inda Camino | **Edición general** Carlos Silva Caffi | **Revisión y edición de contenidos** Hernán Espinoza Medina |**Contenido** Ramón Rivera Notario | **Diseño** Patricio Quezada Andaur | **Corrección de estilo** Carolina Covarrubias Escudero | **Contacto csirt-comunicaciones@interior.gob.cl |** Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, **CSIRT de Gobierno**.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Preguntas sobre cuándo reportar y a quién

- *Pregunta*: ¿Las municipalidades están obligadas a notificar?

R: Sí. Las municipalidades también tienen la obligación de informar y les aplica este decreto. No solamente a la Red de Conectividad del Estado. Le pueden hacer incluso la consulta a la contraloría, interna o regional.

Según el decreto mismo, aplica a "los Ministerios y demás organismos de la Administración centralizada y descentralizada del Estado."

En complemento la ley 18.575[1] señala que "La Administración del Estado estará constituida por los Ministerios, las Intendencias, las Gobernaciones y los órganos y servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad Pública, los Gobiernos Regionales, las Municipalidades y las empresas públicas creadas por ley."

- *Pregunta*: ¿Se deben reportar solo incidentes o todo lo que ocurre, como eventos, por ejemplo?

R: Hay una característica relevante de lo que es un incidente que debe ser notificado y tiene que ver con la existencia de **afectación**, o sea, que se ve alterada ya sea la confidencialidad, la integridad o la disponibilidad del servicio o activo de información. Y claro, están los otros, los eventos, que a nosotros también nos es útil que los reporten. Ustedes nos pueden informar de que les llegó, por ejemplo, un correo de phishing, donde no hubo afectación, no es un **incidente**, porque nadie lo abrió. Pero de todas formas nos sirve que nos envíen la evidencia para extraer y compartir los indicadores de compromiso y crear esta "vacuna" para el resto del sistema. Ese reporte lo necesitamos.

Es así como ustedes deben seguir contribuyendo con esa información. Pero no todo lo que se reporta al CSIRT son incidentes. La **notificación** corresponde en aquellos casos donde explícitamente existe **afectación**, un impacto sobre sus servicios y trabajo. Un impacto en la disponibilidad de sus servicios al público. **Ese es el incidente que se debe notificar**.

En los casos en que ustedes saben que el incidente se debió a un error humano, queda a su criterio si lo notifican o no. Lo pueden **reportar**, señalando que cometimos un error, que existe una indisponibilidad momentánea y la estamos subsanando. Pero si ustedes no saben lo que ocurrió, eso sí debería entrar como **notificación**. Después, en la medida que vayan obteniendo mayor información y si corresponde, pueden informarnos de que era un problema interno que fue reparado.

Cuando nos refiramos a definiciones, tengamos un punto de referencia común. La ISO 27.000 define evento, evento de seguridad, incidente de seguridad, y en base a esto, es claro que una sucesión de eventos puede constituir un incidente. Y **no todo incidente se notifica, solo aquellos que tengan algún tipo de impacto**. Pero una sucesión de eventos puede pasar a constituir un incidente. Debieron ocurrir varios eventos en el camino para que finalmente se produzca un incidente como el *hackeo* de un sistema. En casos así, no se reportan los eventos, se reporta el incidente agregado, que compila un conjunto de eventos, los que desencadenaron en un *hackeo*.

[1] https://www.bcn.cl/leychile/navegar?idNorma=191865

En definitiva, si no tienes claro al principio como se produjo, pero tienes claro que existe una afectación, debes cumplir lo que dice el decreto y notificar al CSIRT de lo que está ocurriendo antes de tres horas desde que fue detectado.

- *Pregunta*: ¿Qué pasa con el spam? ¿Hay que reportar los 500 spam?

R: Apelamos al espíritu del decreto, que está en los considerandos la ley de delitos informáticos y los que hacen referencia al estatuto administrativo, porque existe como obligación funcionaria la de denunciar un delito. Y se menciona el concepto de "afectación". Un spam es un problema de ciberseguridad, pero está siendo controlado por tus herramientas, por lo que no debería ser notificado. Distinto es si uno de esos correos spam logra atravesar esas barreras y un usuario cae en ese engaño y activa una acción maliciosa. Ese sí sería un incidente que genera una afectación y habría que notificarlo.

- *Pregunta*: Qué pasa si el sitio está caído por varias horas y eso es por fallas de configuración u operacionales. ¿Es un incidente que debería reportar?

R: Salvo que tú tengas los elementos o evidencias fundadas de que no hay un hecho delictivo o sabotaje interno, eso queda dentro de la institución. De todas formas, sería bueno que lo reportaras, porque si no lo vamos a ver nosotros y te empezaremos a reportar que tu sitio está caído.

Lo que puedes invocar es que hasta que no tengas 100% de seguridad de que esto no fue un sabotaje interno, puedes reportarlo igual, porque es una falla anormal, puede haber una presunción de un posible acto doloso por terceros o internamente.

- *Pregunta*: Los jefes de servicio, ¿a qué te refieres con jefe de servicio?

R: El jefe de servicio se interpreta literalmente como la más alta autoridad de tu institución. La idea es que no pueda ser que el jefe de servicio no esté informado cuando haya un incidente de ciberseguridad. En toda institución hay cadenas de delegación de funciones, eventualmente la función de ciberseguridad puede estar delegada en un subrogante.

Basta recordar que el Instructivo Presidencial N°8[2] llamaba a designar un encargado de ciberseguridad como responsable de la seguridad informática de institución, pero nunca dejar de mantener informado al jefe de servicio. Porque a él se le va a preguntar, si es que pasó algo, qué se hizo en esa situación. Si el declara que no fue informado, la cosa se complica para toda la cadena de responsabilidad.

Operacionalmente el encargado de ciberseguridad, o a quién se le haya delegado en tu servicio la responsabilidad, puede hacer la notificación, pero el jefe de servicio debe estar enterado de la situación. Porque Interior va a llamar al jefe de servicio.

[2] https://digital.gob.cl/biblioteca/regulacion/instructivo-presidencial-no8-ciberseguridad/

- *Pregunta*: Respecto del rol del jefe de servicio. Yo soy la encargada de ciberseguridad, y en alguna ocasión informamos de eso al CSIRT. ¿Hay que formalizar de forma adicional el que yo estoy encargada de notificar los incidentes?

R: Entendemos que queda implícito en tu resolución de nombramiento como encargada de ciberseguridad. Es importante que esté formalizado en forma de resolución o infraestructura documental según lo que determine cada organización.

- *Pregunta*: Mi relación llega solo hasta la subdirectora. ¿Ahora, yo debería decirle a la subdirectora que debemos informar a la directora? ¿Es una actividad adicional que yo debería realizar?

R: Exactamente. Debieras sumar eso a la cadena. Porque el Ministerio del Interior va a contactarse con la directora, y no puede ser que no esté enterada.

- *Pregunta*: Por favor, entreguen orientación sobre cómo abordar el artículo 3 para dar cumplimiento al decreto.

R: Lo que se busca con esto es (reforzar el) que los jefes de servicio tienen un rol muy importante que jugar. Y de aquí en adelante, los contratos que celebre la organización con los proveedores deben ajustarse a eso.

En estricto rigor, el decreto manda al jefe de servicio a que tiene la obligación de crear esta exigencia. No se lo dice a ustedes, se lo dice al jefe de servicio. Pero esta herramienta puede, quizás, ayudar a mejorar las condiciones de ciberseguridad de la propia organización. Diciéndole al jefe de servicio sabe qué, existe esta responsabilidad administrativa y es suya. Y eso puede ayudar a pedir más presupuesto para cumplir con esta obligación. Porque hay que empezar a exigir, no puede celebrarse un contrato sin contemplar estos elementos. Los contratos nuevos tienen que contemplarlo. Es una obligación, no es una sugerencia. En ese sentido ustedes tienen aquí y en varios decretos ciertas formas de pedir más recursos para mejorar las condiciones y las relaciones en que trabajan con los proveedores y las propias de la organización.

Tienen que verlo también como una oportunidad.

2. Preguntas sobre la necesidad de notificar en tres horas

- *Pregunta*: Qué pasa con las 3 horas para notificar, con los servicios que no tienen personas 24/7 a cargo de su seguridad.

R: Las horas empiezan a contar desde que ustedes toman conciencia de que ocurrió esta situación. Si no hay personas a cargo el fin de semana y el lunes se dan cuenta, desde ese minuto empiezan a correr las 3 horas. Esto no busca forzarlos a tener monitoreo 24/7.

- *Pregunta*: Nos dicen que tres horas para reportar. Pero hay instituciones donde proveedores externos tienen el control, el dominio completo de la estructura y sus componentes. ¿Qué pasa si este proveedor detecta un incidente y la reporta por correo en un horario no hábil, y los responsables dentro de la institución nos enteramos pasadas las tres horas? ¿Cómo se maneja eso?

R: Las tres horas son desde que la organización toma conocimiento. Ahí empiezan a correr las tres horas. Si el proveedor de servicio se enteró, no sé, un sábado, e informó un lunes, el lunes tú tomaste conocimiento. Lamentablemente es así.

- *Pregunta*: Hemos tratado de lograr que los proveedores externos nos comuniquen las vulnerabilidades que presentan sus sistemas, pero de vuelta se nos vienen aumentos de los costos de los servicios, así como también internamente, si sucede un incidente significa horarios, turnos o recursos

R: Efectivamente va a ser así. Pero es absolutamente necesario ir elevando la responsabilidad de los proveedores en cuanto a la seguridad de la información de los activos y los servicios que le prestan al Estado. Y eso se tendrá que traducir, probablemente, en algún incremento en los costos. Por eso en los futuros contratos hay que tener en cuenta la incorporación de estas exigencias, obviamente sujeto a los marcos presupuestarios. Hay que ir sumando e incorporando esos probables mayores costos dentro de la provisión presupuestaria para el próximo año. Esto es necesario. Hay que elevar el estándar.

3. Otras preguntas no relacionadas con el Decreto 273 de 2022

- *Pregunta*: Respeto de la frase "cuando uno observa un hackeo de otro, uno aprende mucho", ¿cómo el CSIRT materializa esto? Hasta ahora nos hemos enterado de incidentes de algún OAE, sin embargo, no se reporta o explica la situación.

R: Queremos empezar a hacerlo. La idea es poder elaborar documentos con las lecciones aprendidas y distribuirlos. Además, la idea es generar una comunidad de práctica con todos ustedes, que involucra más actividades.

- *Pregunta*: ¿Se podría realizar un simulacro de ejercicio de los ataques más frecuentes?

R: El CSIRT organiza simulaciones de ataques. Entiendo que se están organizando un par para este año. Entiendo que se publicará información sobre eso cuando venga.

- *Pregunta*: En base a lo que se quiere regularizar en ciberseguridad, ¿esto incluye que cada organismo posea una unidad dedicada a la seguridad de la información (cargos y personal dedicado)?

R: La obligación (que viene del Instructivo Presidencial N° 8) es que haya un encargado de seguridad, no necesariamente un área.

- *Pregunta*: ¿Se está considerando capacitación para este año, ya sea cursos o diplomados al respecto para quienes no pudimos participar?

R: Intentaremos organizar nuevas iniciativas de educación.

- *Pregunta*: ¿Habrá alguna mesa de trabajo donde integren a los encargados de seguridad de la información o ciberseguridad de las instituciones para implementar las buenas prácticas o normativas para los OAE?

R: Sí, queremos armar una iniciativa para los encargados de seguridad.

- *Pregunta*: Muchas instituciones no tenemos el expertise para detectar una falla de seguridad fuera de lo evidente. Ante una sospecha, ¿uno puede recurrir al CSIRT?

R: Claro, el CSIRT te puede ayudar en esa fase. Cualquier cosa sospechosa la puedes compartir con el CSIRT y un analista te puede ayudar para confirmar la presencia de un actor malicioso, o si se ha vulnerado la seguridad de la institución. Siempre tengan en cuenta, evidentemente, que somos un recurso finito con pocas personas.

Es importante también que tengan sus sensores, que tengan logs, que levanten auditorías. La fase uno es que tengamos esos logs, después veremos quién los revisará, hay que poner automatización, para encontrar anomalías. Ciertamente, están las puertas y los teléfonos abiertos del CSIRT para apoyarlos en este tipo de situaciones.

- *Pregunta*: ¿El CSIRT tiene algún sistema que nos pueda recomendar y ayudar a implementar, herramientas que sirvan para el monitoreo y otras cosas, para que nos podamos preparar?

R: Vamos a tratar de generar alguna línea en esa dirección, como pueden ser paquetes de herramientas, vamos a tratar de recogerlo.

- *Pregunta*: ¿Respecto de los informes de vulnerabilidades, el CSIRT hace algún seguimiento para saber si fueron mitigadas?

R: Hubiera sido ideal que hubiera quedado alguna exigencia de plazo para resolverlo, pero si bien parchar un server o un aplicativo puede ser simple, otros casos no son tan sencillos, necesitando de tiempo y recursos. Si se pusiera un plazo, para algunas vulnerabilidades va a ser muy poco. Entonces, queda a criterio de la institución.

Si ocurre después algo grave, tu habías sido informada de la vulnerabilidad, y no hiciste nada, la responsabilidad administrativa va a recaer sobre ti. Pero si puedes responder que no, que te llegó el reporte y escalaste el tema, pediste los recursos y se te negaron. Nadie está llamado a lo imposible. Pero al menos tú hiciste todos tus esfuerzos por tu parte, desde el punto de vista administrativo. Agotaste todas las posibilidades.

Tenemos que saber escalar estos temas, y traducir nuestros problemas a un lenguaje que el jefe de servicio entienda. Y más importante aún, que entienda el riesgo detrás de no hacer alguna acción mitigatoria respecto de lo que se está reportando.

- *Pregunta*: Con Entel no podemos acceder al monitoreo de tráfico en los switch. El tráfico que se ve es a la salida de cada edificio. He preguntado si podemos levantar un monitoreo y me han dicho que no. ¿Podemos presionar a la gente de Entel para que nos den los monitoreos, por último, los levantamos nosotros?

R: Debiera resolverse del punto de vista contractual. Si lo que me dices está en el contrato, vamos por una modificación del contrato. Eso hay que resolverlo contractualmente. Entel debería abrirles la posibilidad de realizar dicha actividad por parte de ustedes, en atención a que lo pueden levantar fácilmente con herramientas de código abierto.

- *Pregunta*: ¿Hay lineamientos para que tengamos las mismas herramientas, y si hay contratos madres tengamos precios preferenciales para adquirir ciertas plataformas?

R: Entendemos que no, hay libertad de uso de las herramientas, nosotros podemos recomendar una serie de herramientas y cada servicio elegir las suyas. Si es importante que intercambien información de una forma estandarizada, para que puedan conversar. Por ejemplo, que hablen STIX. Que haya interoperabilidad y que todos manejemos correctamente los niveles de confidencialidad TLP.

- *Pregunta*: Por el tema de vulnerabilidades. Cuando aparecen bugs en sistemas operativos en algún equipamiento, y hay que pagar para acceder al parche, ¿hay alguna inversión o presupuesto al que podamos acceder en estos casos?

R: Entiendo que la estrategia es incorporar en los contratos, cuando se compra un dispositivo, debes incorporar la mantención de ese sistema. Es así hasta el minuto.

- *Pregunta*: ¿Entel tiene planes de actualizar sus dispositivos?

R: El espíritu es que, en las próximas negociaciones de contrato, en los contratos se incorporen esos requerimientos. Que cuando contrates un servicio la seguridad esté incluida. Porque si no está mencionado explícitamente en el contrato, los proveedores no lo van a hacer. Por eso se abre en el decreto esa posibilidad. Para que en futuras renegociaciones se incluya el tema desde cero.

- *Pregunta*: ¿Cuándo nos entregan un informe que indica que un sistema no tiene vulnerabilidades, se podría considerar "seguro"? Si después sucede un incidente, pero ustedes indicaron previamente que el sistema no tenía vulnerabilidades, ¿qué significaría eso?

R: Lo que se entrega no es un sello de 100% de seguridad, sino que una visión sujeta a herramientas comerciales, de calidad, que identifican las principales vulnerabilidades. Siempre puede quedar alguna vulnerabilidad no detectada, y precisamente las más críticas se les pasan hasta a las grandes casas desarrolladoras, son las vulnerabilidades de día cero. Esas van a seguir ocurriendo y no son detectadas por las herramientas ni por el ojo de los expertos. No te podemos entregar una garantía de 100% de seguridad.

Lo que implica esto es que siempre debe haber monitoreo y se debe volver a revisar cada tanto período de tiempo. No hay problema en si pediste que te hiciéramos un monitoreo, en tres meses nos lo vuelvas a pedir.

También nos pueden pedir apoyo cuando estén gestando el proyecto y tengan las primeras versiones de prueba. Ahí hacer algún test de seguridad. Porque ahí tienes a todos tus recursos de desarrollo concentrados en el sistema. Es muy distinto y más caro cuando detectas en producción un problema y tratar de corregirlo, porque implica reactivar tu esquema de desarrollo.

- *Pregunta*: ¿Existe alguna forma de saber cuántos reportes recibe el CSIRT por organización?

R: Podríamos informarle a tu organización. Pero no lo del resto. Enviar el requerimiento a csirt-comunicaciones@interior.gob.cl.

- *Pregunta*: ¿Tienen algunas actividades mínimas en el contexto de un plan de crisis que puedan sugerir como buena práctica?

R: Estamos justamente trabajando en ese plan para hacerlo disponible a las instituciones, porque efectivamente no están estandarizados los pasos mínimos ante una situación de crisis. Y eso es clave. Estamos trabajando en eso.

- *Pregunta*: Y sobre el grupo de WhatsApp que mencionan, ¿cuál es y cómo podemos formar parte?

R: Es un grupo de encargados de ciberseguridad y TI. Envíanos tus datos a csirt-comunicaciones@interior.gob.cl y te sumamos sin problemas.

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA
MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA
SUBSECRETARÍA DEL INTERIOR
https://www.csirt.gob.cl/
Teatinos 92 piso 6 Santiago, Chile
Teléfono 1510

CSIRT
Gobierno de
Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.11.08 12:34:20 -03'00'

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática