| *Source* | *Target* |
|---|---|
| Notices<br>This document is provided for informational purposes only. | Avisos<br>Este documento se proporciona únicamente con fines informativos. |
| It represents the current product offerings and practices from XXXX Web Services (XXXX) as of the date of issue of this document, which are subject to change without notice. | Constituye una representación de las ofertas de productos y de las prácticas actuales de XXXX al momento de publicación del presente documento, las cuales están sujetas a modificaciones sin previo aviso. |
| Customers are responsible for making their own independent assessment of the information in this document and any use of XXXX products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. | Los clientes son responsables de realizar una evaluación independiente de la información que aquí se presenta y del uso que le dan a los productos o servicios de XXXX, los cuales se proporcionan “en su estado existente”, sin garantías de ningún tipo, expresas o implícitas. |
| This document does not create any warranties, representations, contractual commitments, conditions, or assurances from XXXX, its affiliates, suppliers, or licensors. | En el presente documento, no se establece ninguna garantía, declaración, compromiso contractual, condición ni promesa de parte de XXXX, sus empresas afiliadas, proveedores o licenciantes. |
| The responsibilities and liabilities of XXXX to its customers are controlled by XXXX agreements, and this document is not part of, nor does it modify, any agreement between XXXX and its customers. | Las responsabilidades y obligaciones de XXXX frente a sus clientes se rigen por los acuerdos celebrados con XXXX, y este documento no forma parte de ningún acuerdo entre XXXX y sus clientes, ni lo modifica. |
| Ransomware: A formidable threat | *Ransomware*: una amenaza formidable |
| Since the first recorded ransomware attack in 1989 called PC Cyborg, ransomware has become a prominent cyber threat featuring dangers that sound more like the stuff of comic books continuing to attract worldwide attention (CryptoLocker [2014], Petya [2016], WannaCry [2017], NotPetya [2017], and Ryuk [2019]). | Desde el primer ataque que se registró, allá por 1989, el cual recibió el nombre de PC Cyborg, el *ransomware* se ha vuelto una amenaza cibernética notoria que encarna peligros que recuerdan a tramas de cómics y que no dejan de capturar la atención de personas de todo el mundo (CryptoLocker [2014], Petya [2016], WannaCry [2017], NotPetya [2017], and Ryuk [2019]). |
| Ransomware attacks are {1>costing governments, nonprofits, and businesses billions of dollars<1}, and interrupting operations. | Los ataques de *ransomware* le {1>han costado a los Gobiernos, organizaciones sin fines de lucro y empresas miles de millones de dólares<1} e interrumpen sus operaciones. |
| Attacks like NotPetya forced shipping giant Maersk to reinstall 4,000 servers and 45,000 PCs for $300M due to “serious business interruption.” | Ataques como NotPetya forzaron al gigante de transportes Maersk a reinstalar 4000 servidores y 45 000 computadoras en lo que significó un desembolso de 300 millones de dólares producto de “una grave interrupción de sus operaciones comerciales”. |
| The ransomware attack on the City of Baltimore cost over $18M, and local governments from Riviera Beach and Lake City, Florida will pay hackers $1M | El ataque de *ransomware* del que fue víctima la ciudad de Baltimore le supuso un gasto de 18 millones de dólares, y los Gobiernos locales de Riviera Beach y Lake City, estado de Florida, le pagarán 1 millón de dólares en total a |

| | |
|---|---|
| combined to hopefully get its systems and data back. | hackers con la esperanza de poder restablecer sus sistemas y recuperar los datos robados. |
| Even though it is difficult to estimate the frequency of ransomware attacks due to an unknown number of unreported incidents and thwarted attacks, the U.S. | Si bien es difícil calcular la frecuencia de los ataques de *ransomware* debido a que un número desconocido de ellos no se denuncian o se ven frustrados, |
| Federal Bureau of Investigation (FBI) anticipates the threat to become "{2>more targeted, sophisticated, and costly<2}" in the foreseeable future. | el Buró Federal de Investigaciones (FBI) de los EE. UU. prevé que estas amenazas serán "{2>más personalizadas, sofisticadas y costosas<2}" en un futuro cercano. |
| These warnings reach beyond U.S. borders, with Europol also calling ransomware the "{3>most widespread and financially damaging form of cyberattack<3}." | Estas advertencias no solo se han expresado dentro de los EE. UU., sino también en Europa, donde la Europol ha catalogado al *ransomware* como "{3>la forma de ciberataque más extendida y destructiva a nivel financiero<3}". |
| What is ransomware? | ¿Qué es el *ransomware*? |
| Ransomware is malicious code designed by cyber criminals to gain unauthorized access to systems and data and encrypt that data to block access by legitimate users. | El *ransomware* es un tipo de código malicioso diseñado por cibercriminales con el objetivo de acceder sin autorización a sistemas y datos, y cifrar estos últimos a fin de impedir el acceso a usuarios autorizados. |
| Once ransomware has locked users out of their systems and encrypted their sensitive data, cyber criminals demand a ransom before providing a decryption key to unlock the blocked systems and decrypt data. | Una vez que el *ransomware* impide el acceso de los usuarios al sistema y cifra su información confidencial, los cibercriminales exigen un rescate a cambio de la clave de descifrado, la cual permitirá liberar el sistema bloqueado y recuperar los datos. |
| In theory, if the ransom is paid within the allotted time, systems and data are decrypted and made available once again and normal operations continue. | En teoría, si el rescate se paga dentro del período concedido, los sistemas y los datos se descifrarán y se habilitarán nuevamente, y las operaciones seguirán su curso normal. |
| However, if the ransom is not satisfied, organizations risk permanent destruction or public-facing data leaks controlled by the attacker. | Sin embargo, si no se paga el rescate, las organizaciones corren el riesgo de desaparecer permanentemente y de que sus datos se divulguen mediante filtraciones controladas por los atacantes. |
| Ransomware does not care | El *ransomware* no discrimina |
| Most ransomware attacks are opportunistic in nature, meaning that ransomware indiscriminately infects any accessible networks through human and/or machine vectors. | La mayoría de los ataques de *ransomware* son oportunistas por naturaleza, lo que significa que infectan de forma indiscriminada a cualquier red a la que pueda acceder a través de vectores humanos o computarizados. |
| It does not matter what industry or geography you are in, as virtually every industry globally has an example of a ransomware incident. | No importa en qué sector o ubicación geográfica se encuentre, existen testimonios de casos de *ransomware* en prácticamente todos los sectores a nivel mundial. |
| However, there is a growing trend amongst bad actors to target certain industries where the probability of successful entry and payout is high. | Sin embargo, hay una tendencia cada vez mayor de dirigir los ataques a sectores en los que la probabilidad de una irrupción y un rescate exitosos son mayores. |

| | |
|---|---|
| Security teams for education institutions, state and local governments, and healthcare organizations are ramping up measures to keep their data safe {1>from an increase in ransomware attacks<1}. | Los departamentos de seguridad de las instituciones educativas, Gobiernos locales y estatales y organizaciones de sanidad están apresurándose en la adopción de medidas para mantener sus datos a salvo {1>a raíz del aumento de los ataques de *ransomware*<1}. |
| Bad actors understand how to identify weak spots in industry verticals. | Los actores maliciosos entienden cómo identificar puntos vulnerables en los mercados verticales del sector. |
| For example, many education and government organizations are vulnerable due to a combination of shrinking budgets, perceived gaps in security resources, and legacy IT systems with unpatched vulnerabilities. | Por ejemplo, numerosas organizaciones educativas y gubernamentales son blancos fáciles debido a una combinación de factores, tales como presupuestos en contracción, brechas en los recursos de seguridad y sistemas de TI heredados cuyas vulnerabilidades aún no se han resuelto. |
| Similarly, ransomware may target industries with intolerance for downtime, like hospitals, in hopes of increasing the probability of payout. | Del mismo modo, el *ransomware* podría tener entre sus objetivos sectores que no pueden permitirse tiempos de inactividad, como ocurre con los hospitales, con la esperanza de incrementar la posibilidad de recibir el rescate. |
| Bitcoin, {1>a popular cryptocurrency, has been an ideal method of making ransom payments because it lacks oversight by any governing body and transactions are kept anonymous.<1} | El Bitcoin, {1>una conocida criptomoneda, ha sido un método ideal para concretar pagos de rescates, ya que carece de supervisión gubernamental y las transacciones se llevan a cabo de manera anónima.<1} |
| Why is ransomware effective? | ¿Por qué es tan efectivo el *ransomware*? |
| Security awareness amongst employees is low | Los empleados tienen poco conocimiento de medidas de seguridad. |
| Organizations are not backing up data | Las organizaciones no hacen copias de seguridad de sus datos. |
| Attacks require little skill and result in significant payouts | Los ataques no demandan gran destreza técnica y los pagos de rescate son significativos. |
| Organizations take weeks to patch critical common vulnerabilities and exposures (CVE) | A las organizaciones, les toma semanas corregir las vulnerabilidades y exposiciones comunes. |
| Overburdened technical staff cannot address or anticipate all security gaps | Un personal técnico agobiado no puede atender ni anticipar todas las brechas de seguridad. |
| Multiple vectors or channels are being used in a single attack | Se utilizan múltiple vectores y canales en un solo ataque. |
| To pay or not pay? | ¿Pagar o no pagar? |
| Active debates exist among cyber security professionals regarding the decision to pay or deny ransom payments. | Dentro de la comunidad de profesionales en ciberseguridad, se han instalado debates activos sobre si se deben o no pagar los rescates. |
| Many experts, including the FBI, {1>advise organizations not to pay the ransom<1}, arguing that paying doesn't guarantee that locked systems and data will be made available again and any payments to cyber criminals | Muchos expertos, entre los que se encuentra el FBI, {1>le sugieren a las organizaciones no pagar por los rescates<1}. Los principales argumentos son que el pago no es garantía de que los sistemas bloqueados se habiliten nuevamente y que cualquier forma de pago a los cibercriminales solo continuaría incentivando conductas criminales. |

| | |
|---|---|
| will only continue to motivate nefarious behaviors. | |
| Even though system and data access is not guaranteed after paying the ransom, some organizations take a calculated risk to pay in hopes of quickly resuming normal operations. | A pesar de que el pago del rescate no es garantía de recuperar el acceso al sistema y a los datos, algunas organizaciones asumen un riesgo calculado de pagar con la esperanza de reanudar sus operaciones lo antes posible. |
| By doing so, they hope to reduce potential ancillary costs of attacks, including lost productivity, decreased revenue over time, exposure of sensitive data{2>1<2}, and reputational damage. | Su principal motivación es reducir los potenciales costos asociados de los ataques, como la pérdida de productividad, la disminución de ingresos en el tiempo, la divulgación de información confidencial{2>1<2} y el deterioro de su reputación. |
| The ransomware threat is serious but smart preparation and ongoing vigilance are effective counters against ransomware. | El *ransomware* es una amenaza seria, pero una preparación inteligente y una vigilancia continua son medidas efectivas para contrarrestarlo. |
| The full armor of data security includes both human and technical factors but there are features of the XXXX Cloud that helps to mitigate against ransomware attacks. | La armadura completa de la seguridad de los datos incluye tanto factores humanos como técnicos, pero hay características de la nube de XXX que ayudan a mitigar los ataques de *ransomware*. |
| XXXX is committed to providing you with tools, best practices, and services to help with high availability, security, and resiliency to address bad actors on the internet. | XXXX se compromete a brindarle herramientas, prácticas recomendadas y servicios que lo ayuden en materia de alta disponibilidad, seguridad y resistencia con el fin de hacer frente a los actores maliciosos que merodean por el Internet. |
| As long as cyber criminals continue to find ways to profit from ransomware, many organizational leaders say, | Numerosos líderes de organizaciones aseguran que, mientras los cibercriminales sigan encontrando formas de beneficiarse económicamente del *ransomware,* |
| {1}{2>“it’s not a matter of if but when an attack will occur.”<2} | {1}{2>“ya no será cuestión de preguntarse si se producirá un ataque, sino cuándo ocurrirá ”.<2} |
| 1{1> Including Personally Identifiable Information (PII) and Protected Health Information (PHI).<1} | 1{1> Esto incluye la información de identificación personal (PII), así como la información de salud protegida (PHI).<1} |
| XXXX is purpose-built for security | XXXX se diseñó específicamente para garantizar la seguridad |
| XXXX protects millions of active customers around the world who represent diverse industries with a range of use cases including large enterprises, startups, educational institutions, and government organizations. | XXXX protege a millones de clientes activos en el mundo provenientes de diversas industrias y con una amplia gama de casos de uso, como empresas, *startups*, instituciones educativas y organizaciones gubernamentales. |
| The scale and global reach of these customers gives us broad visibility and deep perspective on cloud security, which we rapidly reinvest back into our infrastructure and services. | La escala y el alcance mundial de estos clientes nos aportan una visión amplia y una perspectiva completa sobre la seguridad de la nube, que rápidamente reinvertimos en nuestra infraestructura y servicios. |
| Security at XXXX starts with our core infrastructure, which is custom built | En XXXX la seguridad comienza por nuestra infraestructura central, la cual está diseñada específicamente para la nube |

| | |
|---|---|
| for the cloud and designed to meet the most stringent security and regulatory requirements in the world. | y para estar a la altura de los requisitos regulatorios y de seguridad más estrictos del mundo. |
| Inherit physical, environmental, and security controls for IT infrastructure | Controles físicos, ambientales y de seguridad heredados para la infraestructura de TI |
| Before migrating to the XXXX Cloud, customers may have been responsible for the entire control set in their security compliance and auditing program. | Antes de migrar a la nube de XXXX, posiblemente recaía sobre los clientes la responsabilidad de controlar los programas de conformidad, seguridad y auditoría. |
| With XXXX, you can inherit controls from XXXX compliance programs, allowing you to focus on securing workloads and the data you put in the cloud. | Con XXXX podrá heredar los controles de sus programas de conformidad, lo que le permitirá centrarse en resguardar la seguridad de las cargas de trabajo y de los datos que introduce en la nube. |
| XXXX helps relieve your operational burden as XXXX operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. | XXXX lo ayuda a aliviar su carga operativa, ya que opera, administra y controla los componentes; desde el sistema operativo *host* y la capa de virtualización hasta la seguridad física de las instalaciones en las que funciona el servicio. |
| Securing systems and data on XXXX is a shared responsibility | Resguardar los sistemas y los datos en XXXX es una responsabilidad compartida |
| When you deploy systems in the XXXX Cloud, XXXX helps by sharing the security responsibilities with you. | Cuando implementa sistemas en la nube de XXXX, comparte las responsabilidades de seguridad con XXXX. |
| XXXX engineers the underlying cloud infrastructure using secure design principles and customers can implement their own security architecture for workloads deployed on XXXX. | XXXX diseña la infraestructura de la nube subyacente con base en principios de diseño seguros y, a partir de ahí, los clientes pueden implementar su propia arquitectura de seguridad a fin de proteger las cargas de trabajo implementadas en XXXX. |
| XXXX is responsible for protecting the infrastructure that runs all of the services offered on the XXXX Cloud. | XXXX se hace cargo de proteger la infraestructura que ejecuta todos los servicios que se ofrecen en la nube de XXXX. |
| This infrastructure is composed of the hardware, software, networking, and facilities that run XXXX Cloud services. | Esta infraestructura está compuesta por el *hardware*, el *software*, las redes y las instalaciones que ejecutan los servicios en la nube de XXXX. |
| The XXXX Cloud services that a customer selects determine the customer's responsibilities. | Las responsabilidades del cliente se determinan en función de los servicios de la nube de XXXX que selecciona. |
| This determines the amount of configuration work the customer must perform as part of their security responsibilities. | Esto determina la cantidad de trabajo de configuración que el cliente debe realizar como parte de sus responsabilidades de seguridad. |
| Customers are responsible for managing their data (including encryption options), classifying their assets, and using XXXX Identity Access | Los clientes son responsables de administrar sus datos (inclusive las opciones de cifrado), clasificar sus activos y usar las herramientas de XXXX Identity and Access Management (IAM) para establecer los permisos apropiados. |

| | |
|---|---|
| Management (IAM) to apply the appropriate permissions. | |
| Customer | Cliente |
| Responsibility for security 'in' the cloud | Responsabilidad por la seguridad "en" la nube |
| Customer Data | Datos del cliente |
| Platform, Applications, Identity & Access Management | Plataforma, aplicaciones, administración de identidades y accesos |
| Operating System, Network & Firewall Configuration | Sistema operativo, configuración de red y *firewall* |
| Client-side Data Encryption & Data Integrity Authentication | Cifrado de datos del lado del cliente y autenticación de la integridad de los datos |
| Networking Traffic Protection (Encryption, Integrity, Identity) | Protección del tráfico de red (cifrado, integridad, identidad) |
| Server-side Encryption (File System and/or Data) | Cifrado del lado del servidor (sistema de archivos o datos) |
| XXXX | XXXX |
| Responsibility for security 'of' the cloud | Responsabilidad por la seguridad "de" la nube |
| Software | *Software* |
| Compute | Informática |
| Storage | Almacenamiento |
| Database | Base de datos |
| Networking | Redes |
| Hardware / XXXX Global Infrastructure | Hardware e infraestructura global de XXXX |
| Regions | Regiones |
| Availability Zones | Zonas de disponibilidad |
| Edge Locations | Ubicaciones de borde |
| Before ransomware strikes | Antes de un ataque de *ransomware* |
| Network hardening and prevention | Fortalecimiento de la red y prevención |
| Adopt a security framework | Adopción de un marco de seguridad |
| Implementing a security framework like the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) will help to set standards for managing and reducing cybersecurity risks for your organization. | La implementación de un marco de seguridad como el Cyber Security Framework (CSF, Marco de Ciberseguridad) del National Institute of Standards and Technology (NIST, Instituto Nacional de Normas y Tecnología) ayudará a fijar normas para administrar y reducir los riesgos en materia de ciberseguridad para su organización. |
| It's a voluntary, risk-based, outcome-focused framework designed to help you establish a foundational set of security activities organized around five functions—identify, protect, detect, respond, recover—to improve the security, risk management, and resilience of your organization. | Este marco voluntario que se basa en los riesgos y se centra en los resultados se diseñó con el objetivo de establecer un conjunto de actividades de seguridad básicas organizadas en torno a cinco funciones —identificar, proteger, detectar, responder y recuperar— que tienen como fin mejorar la seguridad, la administración de riesgos y la resistencia de su organización. |
| The CSF was originally intended for the critical infrastructure sector but has seen endorsements by governments and industries worldwide as a | El CSF se elaboró originalmente para el sector de infraestructura crítica, pero, gracias al aval que ha recibido de parte de Gobiernos y sectores de todo el mundo, se ha posicionado como un punto de partida recomendado para organizaciones de todos los tipos y tamaños. |

| | |
|---|---|
| recommended baseline for organizations of all types and sizes. | |
| Sectors as diverse as healthcare, financial services, and manufacturing use the NIST CSF, and the list of early global adopters includes Japan, Israel, the UK, and Uruguay. | Sectores tan diversos como el de sanidad, servicios financieros y manufactura utilizan el CSF del NIST, y, dentro de la lista de países que implementaron este marco desde su creación, se encuentran Japón, Israel, Reino Unido y Uruguay. |
| Align to the framework | Alineación con el marco |
| The guide, {1>NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the XXXX Cloud<1}, is designed to help commercial and public sector entities of any size and in any part of the world align with the CSF by using XXXX services and resources. | La guía {1>Marco de seguridad cibernética NIST (CSF, por sus siglas en inglés): alineación con el NIST CSF en la nube de XXXX<1} se elaboró con el objetivo de ayudar a entidades del sector público y privado, independientemente de su tamaño o ubicación geográfica, a alinearse con el CSF a través de los servicios y recursos de XXXX. |
| Deploy secure and compliant XXXX infrastructure | Implementación de infraestructura de XXXX segura y conforme |
| NIST's National Cybersecurity Center of Excellence (NCCoE) has published Practice Guides to demonstrate how organizations can develop and implement security controls to combat the data integrity challenges posed by ransomware and other destructive events. | El National Cybersecurity Center of Excellence (NCCoE, Centro Nacional de Excelencia en Ciberseguridad del NIST) ha publicado guías de práctica para mostrar cómo las organizaciones pueden desarrollar e implementar controles de seguridad a fin de combatir los desafíos que plantea el *ransomware* y otros eventos destructivos en materia de integridad de datos. |
| sLearn more about these, and other preventative security capabilities and measures, in the XXXX whitepaper, {1>Ransomware Risk Management on XXXX Using the NIST Cyber Security Framework (CSF)<1}. | Si desea conocer más acerca de estos controles de seguridad y otras medidas y capacidades de seguridad preventivas, consulte el documento técnico de XXXX {1>Ransomware Risk Management on XXXX Using the NIST Cyber Security Framework (CSF)<1} (Administración de riesgos de *ransomware* en XXXX mediante el marco de seguridad cibernética (CSF) del NIST). |
| NIST Cybersecurity Framework | Marco de ciberseguridad del NIST |
| Identify<br>Asset Management | Identifica<br>Administración de activos |
| Business Environment | Entorno empresarial |
| Governance<br>Risk Assessment | Gobernanza<br>Evaluación del riesgo |
| Risk Assessment Strategy | Estrategia de evaluación del riesgo |
| Supply Chain Risk Management | Administración de riesgo en la cadena de suministro |
| Protect | Proteger |
| Access Control | Control de acceso |
| Awareness and Training | Concientización y capacitación |
| Data Security | Seguridad de los datos |
| Information Protection Processes and Procedures | Procesos y procedimientos para proteger la información |
| Maintenance | Mantenimiento |
| Protective Technology | Tecnología de protección |
| Detect | Detectar |
| Anomalies and Events | Anomalías y eventos |
| Security Continuous Monitoring | Monitoreo continuo de la seguridad |

| | |
|---|---|
| Detection Processes | Proceso de detección |
| Respond | Responder |
| Response Planning | Planificación de respuesta |
| Communications | Comunicaciones |
| Mitigation | Mitigación |
| Improvements | Mejoras |
| Recover | Recuperación |
| Recovery Planning | Planificación de recuperación |
| Improvements | Mejoras |
| Communications | Comunicaciones |
| Segment XXXX Virtual Private Clouds (XXXX VPCs) | Segmentación de la XXXX Virtual Private Cloud (XXXX VPC) |
| Network segmentation mitigates local traffic congestion and also improves security by allocating only the resources specific to the user, which significantly diminishes ways for attackers to move laterally within the network. | La segmentación de la red alivia la congestión del tráfico local y mejora la seguridad, ya que solo se asignan los recursos específicos que necesita el usuario, lo que disminuye drásticamente las posibilidades de los atacantes de moverse de forma lateral dentro de la red. |
| You can provision logically isolated sections of the XXXX Cloud where you can launch XXXX resources in virtual networks that you define. | Puede aprovisionar secciones de la nube de XXXX que estén aisladas de forma lógica. En ellas, podrá lanzar recursos de XXXX en redes virtuales definidas por usted. |
| Segmenting XXXX VPCs into isolated components, either by security groups and network access control lists (ACL) so that only necessary traffic is available can reduce ransomware's ability to spread indiscriminately across XXXX environments. | Segmentar las XXXX VPC en componentes aislados, ya sea en función de grupos de seguridad y Access Control Lists (ACL, listas de control de acceso), de manera que solo se habilite el tráfico necesario, puede reducir la capacidad del *ransomware* de diseminarse de manera indiscriminada por los entornos de XXXX. |
| Manage users' access to critical systems and data | Administración del acceso de los usuarios a datos y sistemas críticos |
| Setting strong IAM policies that determine what systems and data are available to individual users, or groups of users, and under which conditions that data is accessible, can limit how widely ransomware is able to access the environment. | Se puede limitar la amplitud del acceso del *ransomware* al entorno mediante la definición de políticas de IAM robustas en las que se determinen qué sistemas y datos se encuentran disponibles tanto para usuarios individuales como para grupos de usuarios, y cuáles son las condiciones para acceder a esos datos. |
| At the user level, XXXX allows you to define fine-grained access control provisions by defining which users or roles have access to certain systems and data. | A nivel del usuario, XXXX le permite definir reglas de control de acceso muy detalladas en las que podrá establecer cuáles usuarios o roles tienen acceso a determinados sistemas y datos. |
| These controls determine which actions can be performed on a given resource in XXXX, allowing users privileges on a "need-to-know" basis based on business needs and job responsibilities. | Mediante estos controles, se dispone qué acciones se pueden realizar en un recurso dado en XXXX, lo que les otorga a los usuarios privilegios en función de la "necesidad", los cuales están basados en las necesidades de la empresa y las responsabilidades del trabajo. |

| | |
|---|---|
| XXXX IAM enables you to manage access to XXXX services and resources securely. | XXXX IAM le permite administrar de forma segura el acceso a los servicios y los recursos de XXXX. |
| Using IAM, you can create and manage XXXX users and groups, and use permissions to allow and deny their access to XXXX resources. | Mediante el uso de IAM, puede crear y administrar los usuarios y los grupos de XXXX, además de utilizar permisos para otorgar o denegar su acceso a los recursos de XXXX. |
| As a best practice, XXXX recommends following the principle of least privilege for internal and external network users. | Como práctica recomendada, XXXX recomienda seguir el principio de privilegio mínimo para usuarios internos y externos de la red. |
| For example, some strains of ransomware are designed to use a system administrator account to perform their operations. | Por ejemplo, algunos tipos de *ransomware* están diseñados para utilizar una cuenta de administrador de sistema para realizar sus operaciones. |
| With this type of ransomware, decreasing user account privileges and terminating all default system administrator accounts can create an extra security roadblock. | En el caso de este tipo de *ransomware,* se puede crear una barrera de seguridad adicional si se reducen los privilegios de las cuentas de usuarios y se anulan todas las cuentas de administrador de sistema predeterminadas. |
| Define, test, and perform data backup and recovery plans | Definir, probar y realizar copias de seguridad de los datos y planes de recuperación |
| Backups are critical in mitigating the impact ransomware can have on your organization. | Las copias de seguridad son elementos esenciales para mitigar el impacto que el *ransomware* puede tener sobre su organización. |
| The most effective deterrent to ransomware is to regularly back up and then verify your systems. | La forma de disuasión más efectiva contra el *ransomware* es crear copias de seguridad de forma regular y luego verificar sus sistemas. |
| By defining your data backup and recovery strategy, you help protect against deletion or destruction of data during a ransomware attack by being prepared to make data stored in a backup readily available in production environments. | Al definir su estrategia de creación de copias de seguridad y de recuperación de datos, se protege contra la eliminación o destrucción de los datos durante un ataque de *ransomware*, ya que está preparado para hacer que los datos almacenados dentro de una copia de seguridad estén disponibles de manera inmediata en entornos de producción. |
| Regular testing of defined backup and recovery plans in a game day scenario can lead to improved response and assurances that the approach is effective. | Llevar a cabo pruebas regulares de los planes de respaldo y recuperación de datos a través de simulaciones puede contribuir a mejorar las respuestas ante un incidente y puede garantizar que el enfoque adoptado sea efectivo. |
| Customers can use services such as {1>XXXX Backup<1} and {2>CloudEndure Disaster Recovery<2} to build and deploy highly available and resilient applications. | Los clientes pueden utilizar servicios como {1>XXXX Backup<1} y {2>CloudEndure Disaster Recovery<2} para crear e implementar aplicaciones resistentes y de disponibilidad alta. |
| Using XXXX Backup, you can centrally configure backup policies and monitor backup activity for XXXX resources, such as XXXX Elastic Block Store (XXXX EBS) volumes, XXXX Relational Database Service (XXXX RDS) | Si utiliza XXXX Backup, puede configurar de forma centralizada las políticas de copias de seguridad y monitorear la actividad de creación de copias de seguridad de los recursos de XXXX, como los volúmenes de XXXX Elastic Block Store (XXXX EBS), las bases de datos de XXXX Relational Database Service (XXXX RDS), las tablas de XXXX |

| | |
|---|---|
| databases, XXXX DynamoDB tables, XXXX Elastic File System (XXXX EFS), and XXXX Storage Gateway volumes. | DynamoDB, XXXX Elastic File System (XXXX EFS) y los volúmenes de XXXX Storage Gateway. |
| If ransomware strikes, CloudEndure Disaster Recovery can spin up the most up-to-date version of your machines within a few clicks to restore system and data availability to users. | Si se produce un ataque de *ransomware*, CloudEndure Disaster Recovery puede instalar la versión más reciente de sus máquinas con unos pocos clics para restablecer la disponibilidad del sistema y de los datos para los usuarios. |
| Considerations for storing data backups | Puntos a tener en cuenta al almacenar copias de seguridad de datos |
| Organizations that can effectively back up data to a specific point in time and rapidly restore it to production environments significantly reduce ransomware's impact. | Las organizaciones que pueden efectivamente realizar copias de seguridad de los datos en un punto específico del tiempo y rápidamente restablecerlos en entornos de producción reducen significativamente los efectos del *ransomware*. |
| Some newer, smarter ransomware variants are designed to search for stored backups and encrypt or delete them to disrupt recovery efforts. | Algunas formas más inteligentes y novedosas de *ransomware* están diseñadas para buscar copias de seguridad almacenadas y cifrarlas o eliminarlas con el objetivo de contener los esfuerzos de recuperación. |
| Multiple copies of backups should exist and they should be stored in isolated, offline locations. | Por tal razón, se recomienda almacenar múltiples copias de seguridad en lugares aislados y sin conexión a Internet. |
| Including {1>recovery point objectives (RPOs)<1} allow you to determine how frequently backups should be performed so the data is current enough to be useful if it's to be placed in an active production environment. | Si se incluyen {1>Recovery Point Objectives (RPO, objetivos de punto de recuperación)<1}, se podrá determinar con qué frecuencia se deberían crear copias de seguridad, de manera que los datos estén lo suficientemente actualizados como para ser de alguna utilidad en caso de que se deban integrar a un entorno de producción activo. |
| Similarly, the recovery plan should have {2>recovery time objectives (RTOs)<2} that establish how quickly backed up information can be retrieved and put into the production environment to resume normal operations. | De igual forma, el plan de recuperación debería contar con {2>Recovery Time Objectives (RTO, objetivos de tiempo de recuperación)<2} que establezcan qué tan rápido se puede recuperar la información respaldada e integrarla a un entorno de producción a fin de reanudar el curso normal de las operaciones. |
| XXXX environments, resources, databases, code, and other data sources will likely have different RPOs and RTOs based on its priority and criticality to the organization's operations. | Muy probablemente, los entornos, recursos, bases de datos, códigos y demás fuentes de datos de XXXX tengan distintos RPO y RTO en función de su prioridad e importancia para las operaciones de la organización. |
| Find and patch vulnerabilities within XXXX workloads | Hallar y revisar las vulnerabilidades dentro de las cargas de trabajo de XXXX |
| Unpatched vulnerabilities are one of the most common ways ransomware infects an organization's environment. | Las vulnerabilidades no resueltas son uno de los elementos que más suele aprovechar el *ransomware* para infectar el entorno de una organización. |
| By rapidly identifying and patching vulnerabilities, organizations can reduce their exposure to ransomware threats by limiting the ways it can get in. | Si se identifican y se revisan rápidamente las vulnerabilidades, las organizaciones pueden reducir su exposición a amenazas de *ransomware*, ya que limitarían las formas en las que puede acceder. |

| | |
|---|---|
| Using {1>XXXX Inspector<1}, you can search XXXX environments for CVEs, assess your instances against security benchmarks, and fully automate notifying security and IT engineers when findings are present. | Con {1>XXXX Inspector<1}, puede analizar entornos de XXXX a fin de determinar si hay CVE, evaluar sus instancias utilizando estándares de seguridad y automatizar completamente el envío de notificaciones a ingenieros de TI y de seguridad cuando se detecten vulnerabilidades. |
| Once the vulnerabilities have been identified, patching tools such as {2>XXXX Systems Manager Patch Manager<2} can help you deploy operating system and software patches automatically across large groups of instances to close exposures. | Una vez que se identifican las vulnerabilidades, las herramientas de revisión, como {2>el administrador de revisiones de XXXX Systems Manager<2}, pueden ayudarlo a implementar revisiones de software y de sistemas operativos automáticamente en grandes grupos de instancias para resolver las exposiciones. |
| During an Incident | Durante un incidente |
| Early detection and automated responses | Detección temprana y respuestas automáticas |
| Automate security incident detection and alerting | Automatización de la detección de incidentes de seguridad y de la emisión de alertas |
| Responding to any cyber incident requires that you're able to detect the threat's existence in the first place. | Para poder brindar respuesta a cualquier incidente cibernético, primero es necesario ser capaz de detectar la amenaza. |
| If ransomware is detected by a ransom demand popping up on the computer screen, it is too late. | Si el *ransomware* se detecta una vez que aparece un mensaje en la pantalla de su computadora en el que se solicita un rescate, ya es demasiado tarde. |
| Early detection of anomalous user behavior or network activity is key to thwarting ransomware threats and initiating incident response processes. | Detectar de manera temprana actividades anómalas en los usuarios y en la red es fundamental para neutralizar amenazas de *ransomware* e iniciar procesos de respuesta ante incidentes. |
| With an understanding of what "normal" looks like in the XXXX environment, security alerts can be automatically configured to send notifications when malicious or unauthorized behaviors are present. | Las alertas de seguridad se pueden configurar automáticamente para enviar notificaciones cuando se esté ante comportamientos maliciosos o no autorizados gracias a que es posible distinguirlos de los comportamientos "normales" dentro del entorno de XXXX. |
| To help identify such threats, XXXX GuardDuty, a threat detection service, continuously monitors and correlates activity within your XXXX environment for malicious or unauthorized behavior to help you protect your XXXX accounts and workloads. | Para ayudar en la identificación de esas amenazas, XXXX GuardDuty, un servicio de detección de amenazas, supervisa y correlaciona continuamente la actividad que ocurre dentro de su entorno de XXXX para detectar comportamientos maliciosos o no autorizados a fin de ayudarlo a proteger sus cuentas y cargas de trabajo de XXXX. |
| The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. | El servicio utiliza *machine learning*, detección de anomalías e inteligencia de amenazas integrada con el fin de identificar y priorizar las amenazas potenciales. |
| Exercise your incident response plan | Puesta en práctica de su plan de respuesta ante incidentes |
| While XXXX provides capabilities to automate policies and procedures in a policy-driven manner to improve detection times, shorten response times, and reduce attack surface, it is | Si bien XXXX proporciona capacidades para automatizar políticas y procedimientos por medio de políticas con el fin de mejorar los tiempos de detección, reducir el tiempo de respuesta y reducir la superficie expuesta a ataques, recae |

| | |
|---|---|
| the customers' responsibility to develop policies and procedures to respond to cyber incidents. | sobre el cliente la responsabilidad de desarrollar políticas y procedimientos para responder a incidentes cibernéticos. |
| During an incident, your incident response teams must have access to the environments and resources involved in the incident. | Durante un incidente, sus equipos de respuesta ante incidentes deben tener acceso a los entornos y recursos involucrados en el incidente. |
| Identify and discuss the XXXX account strategy and cloud identity strategy with your organization's cloud architects to understand what authentication and authorization methods are configured. | Identifique y analice junto con los arquitectos de la nube de su organización cuál es la estrategia que aplican respecto a su cuenta de XXXX e identidad de la nube para entender que métodos de autenticación y autorización están configurados. |
| By simulating incident response scenarios before a real attack, you can validate that the controls and processes you have put in place will react as expected. | Si efectúa simulacros de respuesta ante incidentes antes de que se produzca un ataque verdadero, podrá cerciorarse de que los controles y procesos que estableció reaccionarán de la manera prevista. |
| Using this approach, you can determine if you can effectively recover and respond to incidents when they occur. | Con este enfoque, podrá determinar si puede responder a los incidentes y recuperarse de sus consecuencias de manera efectiva en la medida que estos se produzcan. |
| Report ransomware to authorities | Denunciar ataques de ransomware a las autoridades |
| The FBI encourages organizations to report ransomware incidents to law enforcement. | El FBI exhorta a las organizaciones a denunciar incidentes de *ransomware* ante las autoridades policiales. |
| The Internet Crime Complaint Center (IC3) accepts {1>online internet crime complaints<1} from either the actual victim or from a third party to the complainant and will work with them to determine the best course of action going forward. | El Internet Crime Complaint Center (IC3, Centro de Denuncia de Delitos en Internet) procesa {1>denuncias de delitos en línea<1} directamente de la víctima o de un tercero relacionado con el denunciante y trabaja con ellos para determinar el mejor curso de acción de cara al futuro. |
| Visit Nomoreransom.org | Visite Nomoreransom.org |
| {1>Nomoreransom.org<1} is a collaboration between law enforcement, IT security companies, and international governments with a goal of helping victims of ransomware retrieve their encrypted data without having to pay the ransom. | {1>Nomoreransom.org<1} es un proyecto que nació de la colaboración entre autoridades policiales, empresas de seguridad de TI y Gobiernos internacionales con el objetivo de ayudar a que las víctimas de *ransomware* recuperen los datos cifrados sin la necesidad de pagar por el rescate. |
| Since it is much easier to avoid the threat than to fight against it once the system is affected, the project aims to educate users about how ransomware works and what countermeasures can be taken to effectively prevent infection. | Dado que es más fácil evitar la amenaza que hacerle frente una vez que el sistema resulte afectado, la intención del proyecto es educar a los usuarios sobre el modo de operación del *ransomware* y qué medidas se pueden adoptar para efectivamente evitar la infección. |
| This initiative is open to other public and private parties. | Esta iniciativa está disponible tanto para partes públicas como para partes privadas. |
| Be prepared to share: | Tenga en cuenta que tendrá que aportar: |

| | |
|---|---|
| Victim's name, address, telephone, and email | El nombre de la víctima, su dirección, número telefónico y correo electrónico |
| Financial transaction information (account information, transaction date and amount, recipient details) | Información sobre la transacción financiera (información sobre la cuenta, monto y fecha de la transacción, datos del destinatario) |
| Subject's name, address, telephone, email, website, and IP address | Nombre, dirección, número telefónico, correo electrónico, sitio web y dirección IP del sujeto |
| Specific details on how you were victimized | Datos específicos sobre el delito |
| Email header(s) | Encabezados del correo electrónico |
| Any other relevant information you believe is necessary to support your complaint | Cualquier información que considere necesaria para sustentar su denuncia |
| Recovering from ransomware | Recuperarse de un ataque de *ransomware* |
| Root cause and lessons learned | Causa raíz y lecciones aprendidas |
| Perform root cause analysis | Ejecución de un análisis de la causa raíz |
| In most cases, your existing forensics tools will work in the XXXX environment. | En la mayoría de los casos, sus herramientas forenses existentes serán de utilidad en el entorno de XXXX. |
| Forensic teams will benefit from the automated deployment of tools across XXXX Regions and the ability to collect large volumes of data quickly with low friction using the same robust, scalable services their business-critical applications are built on. | Los equipos forenses se beneficiarán de la implementación automática de herramientas en las regiones de XXXX y de la capacidad de recopilar volúmenes grandes de datos rápidamente con un nivel bajo de fricción utilizando los servicios robustos y escalables sobre los que están diseñadas las aplicaciones que son esenciales para su empresa. |
| {1>XXXX Detective<1} makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities. | {1>XXXX Detective<1} facilita el análisis, la investigación y la identificación rápida de la causa raíz de los potenciales problemas de seguridad o de las actividades sospechosas. |
| XXXX Detective automatically collects log data from your XXXX resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to conduct faster and more efficient security investigations. | XXXX Detective recopila automáticamente datos de registro de los recursos de XXXX y usa *machine learning*, análisis estadístico y teoría de grafos para crear un conjunto de datos asociados que le permite realizar investigaciones de seguridad más rápidas y eficientes. |
| Update security program with lessons learned | Actualización del programa de seguridad con las lecciones aprendidas |
| Documenting and cycling lessons learned during simulations and live incidents back into "new normal" processes and procedures allows organizations to better understand how they were breached—such as where they were vulnerable, where automation may have failed, or where visibility was lacking—and the opportunity to strengthen their overall security posture. | Documentar las lecciones aprendidas durante simulaciones e incidentes reales, e incorporarlas en procesos y procedimientos "estándar nuevos" les permite a las organizaciones entender mejor cómo estos resultaron vulnerados (por ejemplo, en que puntos eran vulnerables, dónde pudo haber fallado la automatización o dónde faltó visibilidad) y les brinda la oportunidad de fortalecer la posición de seguridad general. |
| Conclusion | Conclusión |

| | |
|---|---|
| Ransomware is evolving, but so can your security awareness and preparedness. | Si bien el *ransomware* está evolucionando, también avanza la forma en que usted se prepara y educa para contrarrestarlo. |
| Government agencies, nonprofits, and businesses around the world trust XXXX to power their infrastructure and keep their systems and data secure. | Entidades gubernamentales, organizaciones sin fines de lucro y empresas de todas partes del mundo depositan su confianza en XXXX para ser quien haga posible su infraestructura y mantenga sus sistemas y datos seguros. |
| Using the XXXX services and best practices shared in this guidebook, you can take proactive measures to reduce the likelihood and impact of ransomware in your XXXX environments. | Gracias a los servicios de XXXX y las prácticas recomendadas contenidas en esta guía, podrá tomar medidas proactivas a fin de reducir la posibilidad y los efectos de un ataque de *ransomware* en sus entornos de XXXX. |
| Get started with XXXX | Comience a usar XXXX |
| Learn XXXX fundamentals, connect with the XXXX community, and advance your knowledge with certifications. | Descubra los aspectos fundamentales de XXXX, conéctese con la comunidad de XXXX y enriquezca su conocimiento mediante nuestra oferta de certificaciones. |
| Register for your free account now. | Registre una cuenta gratuita ya. |
| {1>Sign up › <1} | {1>Registrarse ›<1} |
| Have questions or need help? | ¿Tiene preguntas o necesita ayuda? |
| No matter where you are in your journey to the cloud, we are here to help and answer any and all of your questions about XXXX. | No importa en qué parte del trayecto de su traspaso a la nube se encuentre, estamos aquí para ayudarlo y contestar cualquiera o todas las preguntas que tenga sobre XXXX. |
| {1>Contact us ›<1} | {1>Comuníquese con nosotros ›<1} |
| XXXX Resources | Recursos de XXXX |
| {1}{2>XXXX Cloud Security Resources Hub<2} | {1}{2>Recursos de seguridad en la nube de XXXX<2} |
| {3>Aligning to the NIST CSF in the XXXX Cloud<3} | {3>Alineación con el NIST CSF en la nube de XXXX<3} |
| {4>XXXX Well-Architected Framework – Security Pillar<4}{1} | {4>Pilar de seguridad: XXXX Well-Architected Framework<4}{1} |
| {5}{6>Building a Threat Detection Strategy in XXXX<6} | {5}{6>Building a Threat Detection Strategy in XXXX<6} (Creación de una estrategia de detección de amenazas en XXXX) |
| {7>XXXX Security Incident Response Guide<7}{5} | {7>XXXX Security Incident Response Guide<7}{5} (Guía de respuesta ante incidentes de seguridad de XXXX) |
| {8}{9>XXXX GovCloud (US) Regions<9} | {8}{9>Regiones de XXXX GovCloud (EE. UU.)<9} |
| {10>XXXX Compliance<10}{8} | {10>Conformidad de XXXX<10}{8} |
| U.S. | Islas |
| Federal Government Resources | Recursos del Gobierno federal |
| {1>FBI IC3 – File a complaint<1} | {1>IC3 del FBI: presentar una denuncia<1} |
| {2>The Cybersecurity and Infrastructure Security Agency (CISA) publications<2} | {2>Publicaciones de Cybersecurity and Infrastructure Security Agency (CISA, Agencia de Seguridad de Infraestructura y Ciberseguridad)<2} |
| 2022, XXXX Web Services, Inc. or its affiliates. | XXXX Web Services, Inc. o sus filiales. |
| All rights reserved.<br>索引<br>XXXX EFS | Todos los derechos reservados.<br>索引<br>XXXX EFS |

| | |
|---|---|
| Service-level backups | Copias de seguridad a nivel del servicio |
| XXXX Backup | XXXX Backup |
| Makes it easy to centrally manage backups in the XXXX Cloud via console, APIs, or CLI | Facilita la administración centralizada de las copias de seguridad dentro de la nube de XXXX por medio de la consola, las API o la XXXX CLI |
| XXXX RDS | XXXX RDS |
| XXXX EBS | XXXX EBS |
| Service-level snapshots | Instantáneas a nivel de servicio |
| XXXX Storage Gateway | XXXX Storage Gateway |
| XXXX DynamoDB | XXXX DynamoDB |
| User | Usuario |
| Securely control individual and group access to your XXXX resources | Controle de forma segura los accesos individuales o grupales a sus recursos de XXXX |
| Storage | Almacenamiento |
| Development & Management Tools | Herramientas de desarrollo y administración |
| Content Delivery | Entrega de contenido |
| Analytics | Analítica |
| Compute | Informática |
| Messaging | Mensajería |
| Database | Base de datos |
| App Services | Servicios de aplicaciones |
| Mobile | Dispositivo móvil |
| Payments | Pagos |
| Networking | Redes |
| On-Demand Workforce | Personal bajo demanda |
| VPC | VPC |
| IAM | IAM |
| Before an attack | Antes de un ataque |
| Network hardening and prevention | Fortalecimiento de la red y prevención |
| After an attack | Después de un ataque |
| Root cause and lessons learned | Causa raíz y lecciones aprendidas |
| During an attack | Durante un ataque |
| Early detection and automated responses | Detección temprana y respuestas automáticas |
| Before an attack | Antes de un ataque |
| Network hardening and prevention | Fortalecimiento de la red y prevención |
| After an attack | Después de un ataque |
| Root cause and lessons learned | Causa raíz y lecciones aprendidas |
| During an attack | Durante un ataque |
| Early detection and automated responses | Detección temprana y respuestas automáticas |
| Before an attack | Antes de un ataque |
| Network hardening and prevention | Fortalecimiento de la red y prevención |
| After an attack | Después de un ataque |
| Root cause and lessons learned | Causa raíz y lecciones aprendidas |
| During an attack | Durante un ataque |
| Early detection and automated responses | Detección temprana y respuestas automáticas |
| VPC | VPC |
| Route Table | Tablad de enrutamiento |

| | |
|---|---|
| 172.16.0.0 | 172.16.0.0 |
| 172.16.1.0 | 172.16.1.0 |
| 172.16.2.0 | 172.16.2.0 |
| Router | Enrutador |
| Route Table | Tablad de enrutamiento |
| 172.16.0.0 | 172.16.0.0 |
| 172.16.1.0 | 172.16.1.0 |
| 172.16.2.0 | 172.16.2.0 |
| Security Group | Grupo de seguridad |
| Security Group | Grupo de seguridad |
| Security Group | Grupo de seguridad |
| Network ACL | ACL de red |
| (subnet 1) | (subred 1) |
| Network ACL | ACL de red |
| (subnet 2) | (subred 2) |
| Instance | Instancia |
| Instance | Instancia |
| Instance | Instancia |
| Instance | Instancia |
| Internet Gateway | Gateway de Internet |
| Virtual Private Gateway | Gateway privada virtual |